Legal Issues in the Digital Age. 2022. Vol. 3. No. 2.
Вопросы права в цифровую эпоху. 2022. Т. 3. № 2.

**Articles**

*Research article*
УДК 347
DOI:10.17323/2713-2749.2022.2.4.48

# Internet of Things: Issues Related to the Definition

**Bogdan Yurievich Dorofeev**
3 Bolshoy Triohsviatitelsky Pereulok, Room 113, Moscow 109028, Russian Federation. E-mail: ved-intlaw@yandex.ru

**Abstract**

It is well-known the Internet has become an important part of social life, social and interpersonal communication, a convenient form and a necessary condition for the successful functioning of the economy, the media, and civil society. At the same time, developing technologically and functionally, the Internet generates new technical solutions and new opportunities, leading to the formation of new concepts and terms based on the technological properties of the Internet. One of such new solutions is the emergence of the Internet of Things, a complex technological, technical and economic-legal phenomenon. While a comprehensive understanding of the essence of the Internet of Things is still largely being formed, there are already a number of controversial points and issues that require, among other things, scientific and legal discussions. This article is devoted to the concept of the Internet of Things, the analysis of its scope and content, the study of the meaning and purpose of the term "Internet of things", its relationship with related concepts, and its role in law. Based on the study of the concepts of "Internet" and "things" included in the term "Internet of things", considering the Internet of Things as a complex system, the author explores its elements, defining their definitions, goals, revealing the role in this system. According to the results of the study, the author comes to the conclusion that the main content of the analyzed system is managing process carried out using Internet (as an information technology system) and special technical means. Based on this conclusion, based also on the analysis of the essence of the Internet, the term Internet of Things and the approaches presented earlier, the author proposes a generalized definition of the Internet of Things as a software and technological system for distant control of remote objects carried out in the interests of user using the Internet and the technical properties of managed objects that allow electronic data exchange.

**Keywords**

Internet, Internet of Things, Industrial Internet of Things, information, information technology system, remote things managing.

***For citation:*** Dorofeev B. Yu. (2022) Internet of Things: Issues Related to the Definition. *Legal Issues in the Digital Age*, vol. 3, no. 2, pp. 4–48. DOI:10.17323/2713-2749.2022.2.4.48

## Introduction

As digital technologies and Internet relations continue their fast-paced advancement, the stock of terms used to describe the corresponding phenomena, processes and interactions continues to grow. These processes, quite naturally, require a logical and methodological analysis of the new conceptual apparatus, for an accurate explanation of these terms, and for mapping them against other legal concepts pertaining to similar phenomena and relations in a particular national legal system. Apparently, this undertaking requires a systemic and integrated approach that would summarize, harmonize and standardize this new terminology; this tactics seems necessary in every situation when regulators begin to bring under control novel legal institutions and sub-branches of law in the making, but it is especially important when incipient elements of a national legal system are heavily influenced by constructs borrowed from outside.

A case in point is regulating relations pertaining to the so-called "Internet of things" (IoT), which is a complex technological, economic, social and legal phenomenon of our times. Usually this term is applied to the novel technology of remote wireless communication, which, employing the Internet and the special devices in remote objects, enables the sending of electronic commands to remote entities and the receiving of feedback from these entities in real time, as well as electronic communication among remote entities themselves, without a direct human intervention; in other words, this term describes the technology of electronic data exchange among a system and remote entities or among remote entities. This is how one can remote control, for instance, household appliances, equipment, transportation vehicles, public utilities systems, etc. Such concepts as "smart house," "smart city," etc. are some of the examples of application of this technology in real life. Experts estimate that IoT "potentially can generate trillions of dollars worth of economic opportunities… and enable businesses… to simplify their logistics and cut costs…" [Jackson L., 2016].

Little by little the term IoT began to gain currency both in business circles and in individual academic disciplines, from purely technical to economic and legal. Meanwhile, there are more and more debates over the understanding of this term, over its precise meaning and content. So, carrying out a serious legal analysis of IoT as a concept and identifying and exploring its elements and distinguishing features is an undertaking that is well warranted and of great contemporary importance. These questions are the focus of the present article. This writer, sure enough, makes no claims to have exhaustively researched all materials and studies pertaining to the issue, much less to have reached flawless and definitive conclusions; rather, one should regard this study as yet another contribution to the scholarly legal discussion of the subject, focused on just one term — "the Internet of things" (IOT).

In fact, it has been some time since various researchers began to look at legal relations pertaining to the Internet. These issues have been traditionally regarded as a part of information law, which is usually understood as "an array of norms regulating social relations in information sphere that arise from information exchanges and application of information technologies when one exercises the right to search for, receive, transfer, produce and disseminate information or from the efforts to protect information enforcing information security and legal protection of information discipline" [Fedotov M.F. et al., 2019:17]. That said, certain questions regarding the place of information law in the system of Russian law, as well as the relationship between information law and the Internet law, have caused much disagreement; for a more detailed account see [Kozlov S.V., 2016]. Different approaches are currently in the making, including, for instance, the approach to the Internet law as "a separate legal space with distinctive characteristics" [Arkhipov V.V., 2020: 26–29], as "a complex cross-sectoral area of law, as a complex area of law" [Danilenkov A.V., 2014], or "an integrated area of law " [Lovtsov D.A., 2011: 5, 10].

These issues and legal problems related thereto are very important and, sure enough, deserve to be explored separately. This writer just wants to note that he subscribes to the idea that Internet law is an autonomous legal discipline, as well as a complex interdisciplinary area of law, understood "as an array of interconnected legal norms that embraces provisions regulating relations in the virtual space of the Internet and that is located in a separate space within different areas of law (first of all, information law, international private law, and international public law)" [Rassolov I.M., 2009].

Some legal scholars have already pointed certain terminological issues in information law and Internet relations; see, for instance [Naumov V.B., 2018: 32–39]. And indeed, the development of technologies, moving ahead of the national lawmaking, pushes the boundaries of the terminology and the practice, forever causing scholars and practitioners of law to mull over the complicated questions related to formulating new concepts that would reflect the new relations and to approaches to incorporating these concepts into the national legal system. The task of understanding the term IoT is no exception as this term is gaining an ever stronger foothold among scholars and practitioners of law under the impact of the scientific progress in information technologies.

Thus, for instance, the Russian Federation Government in its "Strategy for Promoting Export of Services Until 2025"[1] emphasizes that "…IoT, by now a global phenomenon, is developing quickly…" and, later in the text, refers to IoT as a breakthrough digital technology in the area of information and telecommunication technologies. In the "Strategy for Developing Machine Tool Making Industry until 2035"[2] IoT is regarded as a priority in the area of development of organizational innovations across the globe; in the "Recommended Practices of Statistical Evaluation of the Technological Development Level of the Russian Federation's Economy In General and In Its Separate Sectors"[3], IoT is referred to as a technology that has a great potential for application in many sectors of economy and leads to structural changes in sectors of economy. The term IoT was also referenced in the Russian Federation President's addresses to the Federal Assembly on March 1, 2018[4] and February 20, 2019[5], in a positive context of the need for technological and innovation-driven development.

[1] Approved by Governmental Directive No. 1797-p of August 14, 2019 "On Approving the Strategy for Promoting Export of Services Until 2025" (together with the "Activities Plan for Realizing the Strategy for Developing Export of Services Until 2025") // SPS Consultant Plus.

[2] Approved by Governmental Directive No. 2869-p of November 5, 2020 "On Approving the Strategy for Developing Machine Tool Making Industry Until 2035." // SPS Consultant Plus.

[3] Approved by Order No. 66 of the Economic Development Ministry of February12, 2020 "On Approving the Recommended Practices for Statistical Evaluation of the Level of Technological Development of the Economy of the RF in General and Its Separate Sectors." // SPS Consultant Plus.

[4] Address of the President of the Russian Federation to the Federal Assembly, March 1, 2018 // SPS Consultant Plus.

[5] Address of the President of the Russian Federation to the Federal Assembly, February 20, 2019 // SPS Consultant Plus.

The term IoT is now used in special-purpose bylaws as well. For instance, one of the Bank of Russia's notices [6] refers to IoT as a technology for communication and data exchange (para 11 of the Annex). At the same time, law has yet to provide a definition of IoT, so presently it is bylaws and doctrine that do the job of explaining this term. Meanwhile, legal scholars addressing IoT currently seem to be only shaping approaches to understanding this phenomenon while present discussions of the definitions of IoT do nothing more than cause further debate.

The format of an article does not allow for an exhaustive review of all interpretations and suggested formulations of IoT; author tries to analyze some of legal experts' current opinions on this issue and, relying on this analysis, suggest a platform for further discussion and research, which would hopefully produce a more accurate definition.

The starting point here arguably should be an analysis of each of the two constituent concepts of IoT, namely, the terms "the Internet" and "thing."

## 1. Defining the Internet

Although the term "Internet" is well known and widely used, there is as still no uniform approach to understanding it.

Art. 2 of the model law "Basics of Internet Regulation," adopted by the Commonwealth of Independent States (CIS) Interparliamentary Assembly[7], describes the Internet as a global information and telecommunication network which connects information systems and electric communication networks of different countries via the global address space, is based on internet protocols (IPs) and transmission control protocols, and enables various types of communication, including publication of information accessible to everyone. As we can see, this definition refers to the following elements of the Internet as indispensable: first, networks of information system, second, a software and technology complex (transmission control protocols), highlighting communication as the function of the system uniting these elements. This writer also believes that this approach requires fur-

[6] Notice No. 5634-У of the Bank of Russia of November 25, 2020 "On the List of Technologies Used for Introducing, Creating or Applying Digital Innovations on Financial Markets in Experimental Legal Regimes in the Sphere of Digital Innovation." // SPS Consultant Plus.

[7] The Model Law on the Basics of Internet Regulation (Order 36-9 approved on May 16, 2011 at the 36th plenary session of the CIS Interparliamentary Assembly) // SPS Consultant Plus.

ther elaboration and clarification with regard to the distinguishing features and elements referenced in the description of the term: communications, global address space, Internet protocols, publication of information.

Russian law approaches the Internet as a type of information and telecommunication networks[8]. Art. 2 of the Federal Law of July 27, 2006 No. 149-FZ "On Information, Information Technologies and Protection of Information"[9] (hereinafter referred to as FZ-149) determines the information and telecommunication network as a technological system for transmitting, via communication lines, information, access to which is effected through computing devices.

The above definition highlights such distinguishing features as:

technological system (apparently, a software suite and technical/computing devices);

communication lines integrated into a single system;

users have the option of remote access to the system via hardware — computing devices.

Law, meanwhile, does not provide yet a straightforward definition of "computing devices." The Soviet GOST standard (GOST 15971-90. State Standard of the USSR. Information processing systems. Terms and definitions[10]) refers to computing machines as an array of technical devices enabling the processing of information and delivery of results in such form as needed. The Russian National Classifier of Fixed Assets OK 013-2014[11] defines computing machines as analog and semi-digital machines for automatic processing of data; electronic, electromechanical and mechanical complexes and machines; devices for automating storage, search and processing of data in the process of solving various problems.

---

[8] For instance, in Art. 2 (13) of Federal Law No. 149-FZ of July 7, 2006 "On Information, Informational Technologies, and Protection of Information"; Art.174.2 of the Tax Code of the RF; Art. 1253.1(1) of the Civil Code of the RF; Art.15.3 of Federal Law No. 39-FZ of April 22, 1996 "On Securities Market"; para 6 of the "Rules for Provision of Telematics Services" (approved by Governmental Order No. 2607 of December 31, 2021 "On Approving the Rules for Providing Telematics Services"), etc. // SPS Consultant Plus.

[9] As amended on December 30, 2021 with amendments and additions in force since January 1, 2022. // SPS Consultant Plus.

[10] Approved by Order No. 2698 of the Gosstandart of the USSR of October 26, 1990.

[11] Adopted and put into effect by Order No. 2018 of Rosstandart of December 12, 2014 "On Adopting and Implementing the Russian National Classifier of Fixed Assets OK 013-2014." // SPS Consultant Plus.

The above mentioned definitions of the computing machine have two key distinguishing features in common: technical devices, gadgets, machines, and information processing related to tasks handled by users. Since it seems obvious that the idea of "technical equipment" is wider than the idea of "machine," so computing equipment (computing devices) should possess all of the above mentioned elements and characteristics of computing machines.

Proceeding with the analysis of the term "the Internet," this writer wants to point out that an understanding of the Internet similar to the one contained in Federal Law No. 149-FZ is reflected or elaborated in case law and bylaws as well. In particular, the Internet is defined as:

network of computers united together by telephone or another means of communication[12],

global system of united computer networks based on the Internet Protocol and IP routing; this system is used to disseminate information in different formats and languages[13];

global (international) multitude of independent computer networks interconnected for information exchange based on standard open protocols[14].

These definitions also reference such distinguishing features as computer networks, a common technological system (communication networks with a single standard protocol), information processing capabilities, the user remote access capabilities. The term "computing" in this context presumably indicates that the system has technical devices responsible for its functioning. But unlike the definition in the law, these ones do not em-

[12] Decision No. 1192/00 of the Presidium of the Supreme Arbitrazh Court of the Russian Federation of January16, 2001 in relation to case No. A40-25314/99-15-271 // SPS Consultant Plus.

[13] Letter of the Russian Federal Anti-Trust Service No. AK/24981 of August 3, 2012 "On Advertising Alcohol in the Internet and Print Publications." Stating that Russian law does not provide a definition of the Internet, this letter goes on to argue that "…in the literature, however, the Internet is defined as a global system of united computer networks on the basis of IP protocol and routing of IP packets. Information in different formats and different languages is disseminated through this system." // SPS Consultant Plus.

[14] Para 9 of the instructions for filing the Federal Statistical Survey Questionnaire "Information on the Use of Digital Technologies and the Production of Goods and Services Related to Them" (Annex 1 to Order No. 463 of the Rosstat of July 30, 2021; as amended on December 17, 2021 and revised on March 25, 2022) "On Approving the Standard Federal Statistical Survey Questionnaires for Institutions Working in the Sphere of Education, Academic Research, Innovation and Informational Technologies" with amendments and revisions in force since January 1, 2022".

phasize methods of connecting to the Internet or devices (called in the law "computing equipment") for connecting to it.

Thus, the legislation in general approaches the Internet first of all as a technological system capable of automatically (electronically) processing information while also providing users with a remote access option. So what are this system's constituent elements? It follows from the above formulations that the system consists, in the very least, of software and technological tools of communication. At this point, two questions arise; answers are important for illuminating the meaning and scope of the term "Internet," as well as for further research:

First, is computing equipment (means of access) a constituent element of information and telecommunication networks (that is an indispensable feature of the Internet) or such devices should not be regarded as such? In other words, should the Internet be regarded only as a software-and-technology communication system or does the term encompass technical equipment providing access to it as well? In this writer's opinion, the formulation in Federal Law No. 149-FZ defines the information and telecommunication network precisely as a technological system of communication (that is as a network plus software), while access equipment is mentioned only in the context of specific functions (applications) of the information and telecommunication network, but not as an inherent and indispensable attribute of the term itself (because strictly speaking an information and telecommunication network can exist without an equipment providing access to it). So, considering access equipment (computing equipment providing access) as a part of the Internet is not justified.

Second, does the information and telecommunication network (as the Internet is defined) include any other technical devices which are vitally necessary for the Internet but which at the same time cannot be considered as the computing equipment (means of access) referenced in Federal Law No.149-FZ? In other words, does the Internet itself possess any indispensable material technical devices, irrespective of the presence of users' devices connected to it? One would assume that certain technical devices (objects of the material world) are vitally important for the Internet: these include, for instance, networks of communication lines, telecommunication equipment, servers, routers, gateways, etc. Sure enough, one can imagine a situation when the Internet connection is delivered in a wireless form directly to users' remote access devices, but in this case some other material communication equipment — for instance, satellites, transmitters, etc. — must be recognized as the "delivery tools" (technical devices of the Internet).

Considering this, it would seem fair to conclude that the Internet as a system should include not only a software suite but also devices enabling the system's functioning (which are not, however, access devices). The legislators used an identical approach elaborating a cognate term "information system" in law mentioned, defining it as an aggregation of information contained in the databases and information technologies and technical devices processing this information (Art. 2); so, technical equipment responsible for the system's operational capability are directly referenced in the definition.

So, author believes it is justified to consider the special technical devices directly responsible for the Internet's functioning (operational capability) as a part of the Internet, an element of its internal structure. It would seem therefore justified to include this group of elements in the definition of the Internet as well.

In addition to legislation in a broad sense, definitions of the Internet can be found in academic legal texts as well, with different authors likewise providing different definitions. Here are some of the definitions proposed:

a global network of networks united by common data transmission protocols [Arkhipov V.V., 2020: 110],

a global system of united computer networks for storing and transferring information [Anisimova A.A., Bevzenko R.S., Belov V.A. et al., 2018],

distributed international knowledge base that includes many data stores (information resources, data /knowledge bases) consisting of documents, data, texts and interlinked by a trans-border telecommunication information web or network [Kopylov V.A., 2002],

a computer (information) network which connects, via appropriate technical devices, subjects who enter into legal relations with each other while exercising rights and duties [Rustambekov I.R., 2015: 22-26].

The first and second formulations are arguably focused on technological aspect of the system; the third, on substantive (characteristics of processed information); the fourth, on legal (legal relations among subjects). These approaches, highlighting separate ontological characteristics of the Internet (networking, data processing, a technology of establishing legal relations), do not conflict with the definition of the Internet in law mentioned.

The Great Russian Encyclopedia defines Internet as a global computer network whose many nodes consist of computers and computerized devices which operate in line with uniform rules within autonomous packet-switched networks with different architectures and technical characteristics and are located in different geographical areas [Ilyin V.D., Kharabet K.V.,

2016]. This definition also references technical devices (computers and computerized devices) as an essential distinguishing feature (element) of the Internet, which, in this writer's opinion, adds necessary clarity, in terms of structural elements, to the definition of information and telecommunication network in law mentioned.

It is useful to highlight two key substantive elements referenced in most of the mentioned definitions:

presence of a common network system for transferring information (that is technical tools enabling the network's functioning, including communication and computerized devices) and,

presence of information technologies (software and technology complex);

aggregation of these elements enables reception, transfer and storage of information in electronic format (electronic information processing) in accordance with the system's uniform rules and also enables connection of users' remote access devices to the system.

Perhaps, one can point to other distinguishing features as well — for instance, remote access, technical specifics of communications, the specifics of the software solution (the protocols), special technical and technological requirements to acceptable information formats, specifics of the origination of legal relations arising from interactions among users as legal subjects, etc.; author believes, however, that these distinguishing features issue from the main ones already mentioned and, if we are to examine the essence of the phenomenon under review, they can be regarded as secondary (accessory) features.

In view of the above, combining the legislative and academic conceptual approaches to the Internet and conjoining descriptions of the system's elemental composition and functionality, this writer would argue that the Internet should be regarded as a type of information and telecommunication network: a technological system of computerized devices, whose software and technology operate in accordance with uniform rules, which is intended for electronic information processing and for connecting users' remote devices (hereinafter processing means a sum total of all possible operations with information, including reception, transfer, creation, transformation, storage). Such systemic approach, this writer believes, describes the phenomenon holistically, allowing to combine its elemental composition and overall functionality. This writer will proceed with his argument applying this complex (systemic) understanding of the Internet.

## 2. The concept of thing

Since the legislation does not explain the generic abstract idea of "thing," let's turn to legal doctrine. Legal scholars, too, have been debating the meaning of the term [for details, see for instance [Sklovsky K.I., Kostko V.C., 2018: 115–143]. Without exploring the arguments in detail (such analysis is beyond the scope of this article), let's start off with an established understanding: in Russian law, things are traditionally understood as "all those objects of the material world whose function is to satisfy particular needs and which a person can possess" [Illarionova T.I., Kirillova M. Ya., Krasavchikov O.A. et al., 1985: 180]. So, author will proceed applying the above understanding of things: any material objects that satisfy a person's needs and that a person can possess. It should be emphasized that the concept of property used in the legislation is undeniably much wider than the concept of "thing" (because property includes, inter alia, ownership rights, results of intellectual activity, intangible rights, etc.) — this clearly follows from Art. 128 of the Russian Federation Civil Code[15].

Yet, as the writer is going to show, in some texts "thing" in the context of IoT is not used in the strictly legal sense, its meaning including other types of property or ownership rights, or even objects not recognized as property in Russian law.

On the one hand, many authors tend to consider things in IoT as primarily objects of the material world: "'thing' in the internet of things can refer to a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile with built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network"[16].

At the same time, some authors writing about IoT include into the category of things "virtual things," "virtual objects," "virtual entities," etc. Russian law has yet to provide a legal definition of those; legal scholars are discussing various approaches and points of view on this issue; see for instance [Sinitsyn S.A., 2016: 7–17], which are very valuable for further research. Another line of inquiry to pursue is the term "virtual property": both in the narrow contexts of information objects in computer games,

[15] Civil Code of the RF (part 1), November 30, 1994, Federal Law No. 51-FZ (as amended on February 25, 2022) // SPS Consultant Plus.

[16] Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (accessed: 09.04.2022)

which are subjectively precious for the gamers, and in a wider sense, including other information objects (accounts, scores, conditional bonuses, etc.) see, for instance [Arkhipov V.V., 2020: 207–215].

In addition to the "virtual entity," legal texts also use a cognate term "virtual asset," which is explained in international law as well. Thus, the General Glossary in the FATF International Standards on Combating Money Laundering and the Financing of Terrorism[17] defines the virtual asset as "a digital representation of value (in another Russian translation, 'value' is translated as 'cost' ['stoimost'–Translator][18] that may be digitally traded, or transferred, and can be used for payment or investment purposes"; "virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations." But this explanation does not address the essence of the asset — it is focused solely on a method of transferring an asset's digital representation (it is an asset's "digital representation" that is being traded). This definition of virtual assets can be applied to any abstract object, if this object has a digital representation (digital form) and if such digital representation itself can be a subject of transactions (transfer). In this definition, the sole distinctive characteristic of the virtual asset as such is the term "value"; the objects (virtual assets) as such are not given other economic and/or legal identifiers.

If in the analyzed definition "value" means "cost" [stoimost'], it is likewise unclear which type of cost is that (political economy differentiates between exchange value, use value, etc.; law differentiates between market value, investment value, etc.[19]); in the absence of indications to the contrary, it appears sensible to assume that the value in question is market value, as the one most widely used and most suitable for general evaluation of assets.

So, since value/cost, as is well known, is a variable depending on many volatile market-based and non-market-based factors, a question begs itself: if

[17] International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF. The FATF Recommendations. Adopted by the FATF plenary in February 2012, amended in 2022. Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (accessed: 27.04.2022)

[18] The above mentioned source contains a definition of virtual assets where the word "value" is used: «A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes." This word can be translated into Russian both as "value" (tsennost') and "cost" (stoimost').

[19] See, for instance, Section III of the Federal Evaluation Standard "Objective of Evaluation and Types of Cost," approved by Order No. 298 of the Defense Industry Ministry of May 20, 2015 // SPS Consultant Plus.

the value is zero or even less (as it happens when certain evaluation methods are applied to certain assets) — does the virtual asset continue to exist? The writer assumes that if understood literally, the discussed definition suggests that a virtual asset is based on numerical representation of any value (there are no boundaries set for values); so, it would seem justified to presume that a virtual asset exists even if its value is zero or below zero. Especially since the amount of a cost or a value per se is not an obstacle to transactions involving such asset or other legally significant acts (for instance, actions with financial stakes, such as expecting the value of such asset to grow).

Interestingly, the above mentioned definition of virtual assets is close to the definition of digital currency in Art. 1(3) of the Federal Law of July 31, 2020 "On Digital Financial Assets and Digital Currency, and on Introducing Amendments to Certain Legal Acts of the Russian Federation"[20] (hereinafter referred to as Federal Law No. 259-FZ), where digital currency is "a series of digital data (digital code or reference) contained in the information system that is offered and/or can be accepted as a means of payment not constituting a monetary unit of Russia, a foreign country or an international monetary unit or a payment unit and/or as an investment, and with respect to which there is an obligor liable to each holder of such electronic data, except the operator and/or nodes of the information system required only to ensure that the procedure for the issue of such digital data and for making or changing entries in the information system complies with its rules."[21] As we can see, the formulation in the Russian law references all essential features of the definition of the virtual asset — a digital representation that can be traded (transferred) in a digital form and/or can be used for payments or investment; and, had it not been for the special provision in the FATF Recommendations that the term virtual assets may not be applied to fiat money or other financial assets, digital currency, based on the definitions compared above, could well be considered as a type of virtual assets. For instance, there are already court rulings in which cryptocurrencies are regarded as a type of virtual assets[22].

[20] Federal Law No. 259-FZ of July 31, 2020 "On Digital Financial Assets and Digital Currency, and on Introducing Amendments to Certain Legal Acts of the Russian Federation." // SPS Consultant Plus.

[21] Cited: URL: https://www.debevoise.com/-/media/files/insights/publications/2020/08/20200806-russia-adopts-law-on-digital-eng.pdf. (accessed: 12.06.2021)

[22] For instance, para 1 of Decision No. 32 of the plenary session of the Supreme Court of July 7, 2015, amended on February 26, 2019 "On Case Law Related to Legalization (Laundering) of Financial or Other Assets Acquired Through Crime and on Buying or Selling Assets Known to be Acquired Through Crime." // SPS Consultant Plus.

It should be also pointed out that virtual assets are not the same as digital financial assets. Thus, according to Art. 1(2) of the earlier mentioned Federal Law No. 259-FZ, digital financial assets are digital rights, including "monetary claims, ability to exercise rights attaching to issuable securities, interest in the capital of a non-public joint stock company, and [the] right to require transfer of issuable securities" that were issued pursuant to a decision to issue digital financial assets in the manner prescribed by law and whose issue, recording and trading can be carried out only "by means of making or introducing entries in a distributed ledger-based information system or in other information systems."[23] The law thus provides an exhaustive list of types of rights and claims categorized as digital financial assets. Unlike the approaches to understanding virtual assets and digital currencies, the definition of digital financial assets is clear about substantive characteristics of such assets — such assets not only have a digital form, but, the legislator explains, include property and ownership rights; these types of assets are well known and regulated by civil legislation, and their only new specific characteristic referenced in Federal Law No. 259-FZ is digital representation (and, as an accessory feature, the distributed ledger technology is referenced as one of the possible methods of recording these rights). It is clear that the definition in that Law does not apply to the rest of non-material assets (those that are not directly referenced in the law) and, so, these assets cannot be considered as digital financial assets. Besides, as mentioned earlier, the definition of virtual assets set forth in the FATF Recommendations excludes monetary claims, fiat money, and securities.

And finally, digital financial assets are defined as digital rights, that is "obligations or other rights specifically named as such by law, and their essence and terms for exercising them are provided for by the rules of an information system meeting the requirements set forth by law"[24] — Civil Code, Art. 141.1(1), whereas virtual assets are nothing more than digital representations of the value/cost (of course, if the understanding of virtual assets is based on the approach adopted in the FATF Recommendations mentioned above). And whereas virtual assets from the very beginning can be used, inter alia, for payment, digital financial assets cannot.

[23] Cited: URL: https://www.debevoise.com/-/media/files/insights/publications/2020/08/20200806-russia-adopts-law-on-digital-eng.pdf (accessed: 12.06.2021)

[24] Cited: URL: https://www.debevoise.com/-/media/files/insights/publications/2019/03/20190314_russian_state_duma_adopts_bill_on_digital_rights_in_third_reading_eng.pdf (accessed: 20.04.2021)

It would be hardly justified, therefore, to regard digital financial assets as a type of virtual assets; the rights included in digital financial assets are excluded from virtual assets.

The classical understanding of thing as a material object, therefore, is arguably justified when using the term in legal regulation in general and in definitions of IoT in particular. Describing other elements of the analyzed phenomenon's separate virtual features that are not related to things, one should use a different terminology that does not conflict with the definition of things set out here.

So, concluding this analysis of the concepts of "the Internet" and "thing," before proceeding further, this writer wants to emphasize that legal acts do not elaborate the essence of the concept of IoT. At the same time, IoT is described in some bylaws, as well as in legal scholarship. Let's review some of these formulations.

## 3. Definition of IoT

As follows from para 4 ("в") of the "Strategy for Developing Information Society in the Russian Federation for 2017-2030"[25], IoT is the concept of a computing network connecting things (material objects) that have embedded information technologies enabling these things to interact with each other and with an external environment without human intervention. A similar approach is used in the "Methodological Recommendations for Introducing Modern Digital Technologies in the Core Curriculum of Secondary Schools"[26], which define IoT as the concept of a computing network of physical objects which have embedded technologies for interacting with each other and an external environment, and this concept is underpinned by the belief that the creation of such networks would lead to re-organization of economic and social processes and make human intervention redundant in some actions and operations.

Both of the above definitions recognize IoT as a concept and highlight its functional and technological aspects: a single network, as well as remote things connected to the network thanks to information technologies. As we can see, the new distinguishing feature (that is a feature not pres-

[25] Presidential Decree No. 203 of May 9, 2017 "On the Strategy for Developing Information Society in the Russian Federation for 2017-2030." // SPS Consultant Plus.

[26] Approved by Directive No. P-44 of the Education Ministry of the RF of May 18, 2020 "On Approving the Recommended Practices for Introducing Modern Digital Technologies in the Core Curriculum of Secondary Schools." // SPS Consultant Plus.

ent in the Internet as such) here is the capabilities for things interacting with each other thanks to technical devices and information technologies, without human intervention. And the concept of thing in this approach is close to the legal concept, where things are regarded as material objects. At the same time, this definition does not sufficiently address such aspects as IoT's software and technologies, as well as the IoT environment — in short, the Internet per se as the information and telecommunication network (perhaps it is implied in the phrase "computing network"); besides, in this writer's opinion, such term as "a computing network of physical objects" requires further elaboration too.

The "Traffic Safety Concept for Public Roads with Driverless Transportation Vehicles (DTVs)"[27] defines IoT as "an aggregation of networks of machine-to-machine communications and systems of big data storage (processing) in which various processes and objects (Internet of Things, IoT) become digitized thanks to sensors and actuators (actuating mechanisms) connected to the system." The key distinguishing features referenced in the definition are these:

presence of information (communication) networks,

presence of information processing systems (apparently, software and technology tools),

presence of connected command devices (actuation mechanisms);

presence of the digitizing capability (digitization is usually understood as the execution, in a digital environment, of functions and processes (business processes) previously carried out by people and organizations without the use of digital products[28]).

Whereas the first two features are arguably typical for the Internet in general, the last two clearly highlight new, IoT-specific characteristics. Let's also note that this definition emphasizes communications among machines / machine-to-machine communications (that is "interactions among machines") while adding a direct goal of the "interactions among machines" and the functioning of networks and data: digitization of processes and

[27] Section I of the "Traffic Safety Concept for Public Roads with Driverless Transportation Vehicles (DTVs)," approved by Governmental Directive No. 724-p of March 25, 2020 "On Approving the Traffic Safety Concept for Public Roads with Driverless Transportation Vehicles (DTVs)." // SPS Consultant Plus.

[28] Art. 1(3) of the "Guidance (Recommended Practices) for Developing Regional Projects Under the Auspices of Federal Projects of the National Program 'Digital Economy of the Russian Federation,'" approved by Order No. 428 of the Ministry of Communication of the RF of August 1, 2018 // SPS Consultant Plus.

objects. Digitization also implies a more important common goal — managing processes and objects, although the definition does not specifically emphasize this aspect.

The standard ISO/IEC 20924:2018 "Information technology — Internet of things (IoT) — Vocabulary" (updated in 2018) provides the following definition of IoT: "infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world»[29].

So, in this version of the definition there are four clearly identifiable internal and interconnected elements of IoT:

technological system (systems);

information resources;

remote (autonomous) objects;

software (services);

and a sum total of all the listed elements is called infrastructure, that is IoT is approached as an infrastructure in the first place.

And now regarding such feature as "information resource": although the version of Federal Law No. 149-FZ currently in force does not provide a definition of information resources, the previous piece of legislation, Federal Law No. 24-FZ of February 20, 1995 (revised January 10, 2003) "On Information, Informatization, and Protection of Information" defined information resources, in Art. 2, as separate documents and separate arrays of documents, as well as documents and arrays of documents in information systems (libraries, archives, funds, data banks, other information systems). So, considering that the mentioned Standard does not state otherwise, information resources in this context arguably should be best defined as a variety of information in the form of documents (in this case — electronic documents).

[29] Standard of the International Organization for Standardization ISO/IEC 20924:2018 "Information technology — Internet of Things (IoT) — Vocabulary". Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:20924:ed-1:v1:en (accessed: 21.01.2022). The document contains the following definition: "infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world." (Presently a new version of the standard is effective: ISO/IEC 20924:2021 Information technology — Internet of Things (IoT) — Vocabulary (Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:20924:ed-2:v1:en,(accessed: 21.01.2022) although the text of the new version has not been posted yet on publicly accessible web sites. The definition discussed in this article is the one provided in the previous version of the mentioned Standard (20924:2018).

In the statistical questionnaire "Information on the Use of Digital Technologies and the Production of Goods and Services Related to Them"[30], IoT is understood as interconnected devices, or systems can be remotely controlled via the Internet. This approach highlights the system's general functional description (interconnectedness of devices remotely controlled via the Internet) and emphasizes such distinguishing features as remote control of devices and the presence of a software that makes the system tick — the Internet. Author believes, however, that this definition is incomplete: it does not specify methods and mechanisms of control ("via the Internet network") nor does it reference pivotal features of the devices and systems. Besides, the mentioned control is perhaps not the system's sole objective and function (there is a more detailed analysis of this in part 5 of the article).

Along with the term IoT, scholarly literature and legislation also features its subcategory — that is, "industrial IoT" (IIoT). The introduction of an additional distinguishing feature ("industrial") imparts specificity to a generic term and in this case is supposedly intended to highlight two additional properties of the defined phenomenon: first, a specific purpose (objective) of the use of IoT — entrepreneurial or other professional activity; second, the peculiarities of the "things" themselves — their industrial nature (tools, equipment, machinery, etc.). This writer believes that the mentioned additional features do not provide insight into internal vital features and properties of IoT as a concept, nor do they create an autonomous approach to interpreting IoT's main (essential) elements or change its essence. With this clarification in mind, this writer believes it is justified to further make use of this formulation along with the other definitions of IoT, with certain qualifications.

Thus, according to the annex to the statistical questionnaire "Groups of Advanced Industrial Technologies" [31], the industrial Internet is conceptual-

[30] Line 118 of Section 1 "General Information" of the Federal Statistical Survey Questionnaire "Information on the Use of Digital Technologies and the Production of Goods and Services Related to Them," annex 1 to Order No. 463 of the Rosstat of July 30, 2021; as amended December 17, 2021 and revised March 25, 2022 "On Approving the Standard Federal Statistical Survey Questionnaires for Institutions Working in the Sphere of Education, Academic Research, Innovation and Informational Technologies" (with amendments and revisions in force since January1, 2022)." // SPS Consultant Plus.

[31] Line (code) 3002 of the Annex to the Federal Statistical Survey Questionnaire (background information) "Groups of Advanced Industrial Technologies," Order No. 463 of the Rosstat of July 30, 2021; as amended on December17, 2021 and revised on March 25, 2022 "On Approving the Standard Federal Statistical Survey Questionnaires for Institutions Working in the Sphere of Education, Academic Research, Innovation and Information Technologies" (with amendments and revisions in force since January 1, 2022)."

ized, firstly, as the concept of creation of information and communication infrastructures where industrial devices, equipment, detectors, sensors, process control systems are connected to the information and telecommunication network the Internet, and where data transferred and received by software is integrated without human intervention. The thing in IoT, meanwhile, is understood as an object of the physical world (physical things) or information world (virtual things), which can be identified as an autonomous object and integrated into communication networks. And here again one can see a liberal approach to things in the context of IoT, whereby things are not only things in legal sense but also other types of property, as well as probably other objects whose inclusion into the category of property does not seem to have a clear rationale.

Furthermore, the approach applied in the "Recommended Practices for Introducing and Using Industrial Internet of Things for Optimizing Control (Oversight)"[32] seems noteworthy: defining IIoT, the document's authors first list its instruments and technologies, noting, in particular (para 1.1), that the term IIoT is used to designate an aggregation of the following automatic or automated instruments and technologies:

measuring tools that convert data about external environment into a machine-readable format (measuring tools);

tools for transferring such data from measuring tools to information systems that process it, and from there, to response systems (data transfer tools);

data processing tools, which accumulate and analyze data sent from measuring tools (data processing tools);

response systems, acting in a certain way when data has been processed (response systems);

systems of remote monitoring of the performance of the above mentioned tools and technologies (monitoring systems).

And further in the text, describing how IIoT can be used for control and oversight (para 1.2 of the mentioned "Recommended Practices…"), the document defines it as an aggregation of automatic or automated measuring tools, data transfer and processing tools, remote monitoring systems and response systems, which provide controlling agencies with accurate in-

[32] "Recommended Practices for Introducing and Using Industrial Internet of Things for Optimizing Control (Oversight)" (approved by the protocol of the session "Reforming Control and Oversight" of the Task Force for devising core activities of the Russian Federation's strategic development No. 73. of November 9, 2017 // SPS Consultant Plus.

formation about objects under watch and which are used for the purpose of control (oversight) in accordance with legal acts, standards and regulations approved in the manner as prescribed. If we exclude from this definition references to a special purse (control and oversight), one can identify the following key common features:

presence of a data transfer system (a technological system);

presence of a data processing system (a software suite);

presence of remote management devices (measuring and monitoring);

processes are automated (remote processes).

As we can see, this explication is quite close to the definition, reviewed above, provided in the "Traffic Safety Concept…" approaching IoT as an aggregation of networks of machine-to-machine communication and big data storage (processing) systems that digitize various processes and objects with the use of sensors and actuators connected to the network; only instead of the process of digitization, the "Recommended Practices…" mentions a similar process such as automation (automated devices for process management and data processing). Let's note that the last two features in the formulation from the "Recommended Practices…" highlight key distinctive features of IoT: the presence of remote management devices and the application of a technology of automated (digitized) process management.

Definitions of IoT are provided in some other sources as well — academic and professional literature, specialized web sites. Thus, some authors [Bagoyan E.G., 2019: 42–49]; [Arkhipov V.V., Naumov V.B., Pchelintsev G.A., Chirko Ya.A., 2016: 18–25] grappling with the task of conceptualizing IoT, bring up the Recommendation of the International Telecommunication Union No. 2060 Y. (June 2012), which describes IoT as "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" and provides the following definition of "thing": "with regard to the Internet of things, this 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."[33] One could argue that refer-

[33] Para 3.2.2-3.2.3 of the Recommendation Y.4000/Y.2060 (06/12) of the International Telecommunication Union (ITU) "SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS Next Generation Networks — Frameworks and functional architecture

ences to certain elements and distinguishing features in the above definition are based on a subjective judgment, the meaning of these references is not quite clear and this lack of clarity is an obstacle to understanding the terms correctly: "global," "advanced," "evolving," "the information world" (the definition of the information world, provided in laws and regulations, as a society where information and the level of its use and accessibility have vital impact on citizens' economic and sociocultural living standards[34] is highly subjective.). If the above references to elements and features, which require additional explanation, are excluded, the gist of this definition, in a simpler form, can probably be summed up as follows: IoT is an informational and technological network infrastructure connecting things with each other. It appears that such approach, although emphasizing the connecting of things as the key feature of IoT, still fails to mention the function of this connection — management of things. Perhaps this function is implied in the phrase "enabling advanced services," but due to its lack of clarity one cannot be sure.

Again take note of the obvious expansion of the idea of "thing": in the definition under review it likewise includes "virtual things" and, so, is obviously wider than the legal term "thing" in Russian law.

Some authors focus their attention on technical aspects of IoT as a system of technical devices, understanding IoT as "an aggregation of various appliances, sensors, devices united into a network through any available communication channels and using different protocols interacting with each other and a single protocol for accessing the global web" [Roslyakov A.V., Vanyashin S.V. , Grebeshkov A.Yu., 2015: 7]. These researchers mention the following basic principles of IoT:

an omnipresent communication infrastructure,

global identification of every object,

each object has a capability to send and receive data via a private area network or the Internet, to which it is connected.

Some authors approach IoT as a concept. Thus, for instance, IoT is interpreted as a concept uniting many technologies and implying the use of sensors and the connection of all appliances (and things in general) to the Internet: this arrangement enables remote monitoring, control and

models Overview of the Internet of things". Available at: https://www.itu.int/rec/T-REC-Y.2060-201206-I (accessed: 06.04.2022)

[34] Para 4("r") of the "Strategy for Developing Information Society in the RF for 2017-2030" (approved by Presidential Decree No. 203. May 9, 2017 // SPS Consultant Plus.

management of processes in real time (including automatically) [Keshelava A.V., Budanov V.G., Rumyantsev V. Yu. et al., 2017: 8]. Such approach seems justified for describing a concept as an idea underpinning a phenomenon.

In some professional texts one can find an even wider interpretation of IoT. For instance, as a concept of connection of any device with a switch on/off to the Internet (and/or to other devices) or as a gigantic network of interconnected "things" [Morgan J., 2014][35], which supposedly brings into the spotlight the technological idea underlying the term; however, one can hardly consider such formulation of the phenomenon in question as comprehensive and accurate.

Some authors look at IoT as a system of interconnected computing devices, mechanical and digital tools, objects, animals or people which/who are provided with unique identifiers and enabled to transfer data via a network without the need for humans to interact with each other or with computers[36]. As we can see, in this formulation "things" are substituted with a broader term — "objects"; besides, the system of interconnected elements also includes animals and people, and there are references to important distinguishing features of the system — automation of interaction (without human intervention) and digitization of the processes (unique identifiers, data transfer via network).

What leaps to the eye is the similarity of many of the quoted definitions in the core aspect — references to a network of remote autonomous objects either connected to the common technological system (the Internet) or interacting with each other through it. So, given the terminological and functional closeness of the ideas of IoT and the Internet, it would seem useful to highlight differences between them.

First, one needs to ask whether IoT is a separate type of the Internet, existing outside it in an independent and self-contained system? Obviously not — IoT uses the same software and technology system (platform) of the Internet as the information and telecommunication networks. So, because our understanding of the Internet is based on our approach to it as a technological system (an information and telecommunication networks of a

[35] Available at: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=441defc81d09 (accessed: 09.04.2022)

[36] Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. Tech Target (accessed: 09.04.2022)

certain type), it seems natural to recognize that IoT is a system too. In this context, both ideas have the same elements: IoT, being based on technology and the Internet connection, naturally has all the features of the Internet: a technological system (a communication network with a single standard protocol), the data processing capability, the remote access capability for users.

The Internet is not the only software and technology platform for remote management of remote objects (things). Yes, the Internet here is a type of information and telecommunication networks, enabling exchange and processing of information transferred to and from things within a common software and technology infrastructure. But does the task of managing objects require specifically the Internet — is it feasible without the Internet? One would argue that other communication methods and devices can serve the purpose as well: for instance, radio communication (radio control of objects or sites — for instance, in aeromodelling). Besides, in addition to the Internet, there are other types of information and telecommunication networks (for instance, self-contained corporate communication networks — intranets). Remote management of things, therefore, is possible in other infrastructural and technological configurations too (this writer does not discuss here comparative advantages of the mentioned communication methods but only highlights the existing options) and, so, IoT is just one of the technological instruments of remote management of objects (things), which operates via one of the types of information and telecommunication networks (systems).

As noted in discussion of the idea of IoT, however, this term has some distinguishing features that are absent in the Internet. These features highlight a functional difference of IoT: whereas the Internet's sole functional purpose is to have a unit connected to its system and have information processed in this system, IoT's main function is to impact technological processes and the functioning of remote objects through electronic data exchanges with the special technical devices embedded in these remote objects. That said, such remote objects and devices, as noted above, are not incorporated in the Internet proper (in other words, they are not enablers of the Internet as such).

The mentioned functional differences, therefore, should be matched with differences in the terminology; as was already noted, the key features of IoT (the ones that distinguish it from the Internet per se) are, first, the devices for remote management of objects (sites) — these devices must meet the system's technical standards and be connected to remote objects

(things); and second, the capabilities for automated (digitized) data exchange between the system and the remote devices embedded in such objects and among the remote devices themselves — the capabilities that enable the management of objects. Instruments for electronic data exchange, the mentioned special technical devices for remote management of objects (sites) are referred to in the sectoral legislation as detectors (sensors), actuating elements or actuators[37].

Or, to express it in simpler terms, the key distinguishing features of IoT arguably are a) objects (things) that can be managed remotely thanks to the electronic data exchange technology, and b) the special technical devices embedded in managed objects, which are responsible for electronic data exchange for the purpose of management.

It is precisely these particularities and features that produce the phenomenon called in some formulations of IoT "interaction of things." If we are to get an all-round understanding of the term under review, it is important to analyze the substance of this interaction and evaluate the accuracy of the formulation used to describe this process. Keeping this in mind, it has a sense to study the essence, main features and character of the "interaction of things."

## 4. "Interaction of things" in the system of IoT

Let's make it clear from the start that interaction of things should not be analyzed in the context of their (things') willed actions (deeds). It is clear that inanimate objects cannot act purposefully without an intervention of the human will. Such expression of will vis-à-vis a thing can be effected either directly (an example: mechanical relocation of an object caused by the application of physical force by a person) or indirectly (for instance, by sending remote commands via communication tools or automated mechanisms). Obviously, IoT in any case involves an expression of human will to activate one or another function of remote objects, it is just that in this case this will is expressed when human beings create source codes or algorithms which are put into play via the Internet and the special technical devices embedded in remote objects and which materialize in the form of the remote object's responses — such as, for instance, transferring electronic data to the technical devices embedded in another remote object. This is the process this writer envisions speaking about "interaction of things," al-

[37] Section I of the "Traffic Safety Concept for Public Roads with Driverless Transportation Vehicles (DTVs)," approved by Governmental Directive No. 724-p of March 25, 2020.

though a more accurate descriptive term would be, for instance, "electronic data exchange among the technical devices embedded in remote objects (within an algorithmic framework designed by users)."

The above analysis arguably also shows that saying that things "interact" without human intervention is hardly justified — human intervention is necessary anyway, even though it is limited to installing software and communication hardware — sure enough, a person does not need to apply physical efforts to the thing. Minimization of human intervention is also characteristic for other, IoT-free modes of automated operation of devices and tools — the examples include tools with digital program control, robotized assembly lines and assembly operations, aeromodelling, etc. What arguably distinguishes functioning of remote objects in IoT is, first, the special technical devices embedded in these things, and second, the specific type of electronic communication between them, based on the Internet's technologies and software.

So, what are the devices or objects that "interact" in IoT?

Interaction in this context refers only to things (objects, devices) that are part of IoT but not of the Internet as such. Functionality is what distinguishes IoT's managed things (objects) and objects in the Internet's technological system — let's compare functions and intended use of the Internet and IoT: objects (technical devices) of the Internet are responsible for the operation of the Internet (as an information and telecommunication system), whereas in the IoT environment objects (technical devices) that are categorized as "things" are managed by individual users and their function is to accomplish local specific tasks set by users — tasks that are not related to the general performance of the Internet as an information and telecommunication network. It is not unfathomable that one and the same thing may appear to perform these two functions at once, but if so, this is obviously not because these functions cannot be separated in principle but because what looks like one and the same thing (remote object) can have technically and technologically, several different technical devices serving different purposes embedded in it: in this case, in the given context, perhaps one can talk about two or more devices combined into one complex thing. For instance, a transportation vehicle can provide the services of a personal computer, a router or a server, connecting its passengers to the Internet (in which case this vehicle's relevant elements can be regarded as technical devices of the Internet and computing devices used for accessing the Internet) — and at the same time this vehicle can serve as a vehicle of transportation remotely managed via the Internet and the special technical devices.

Thus, one is led to conclude that the technical devices (elements of the technological system of) the Internet are not the same as things in IoT: the former's purpose is only to keep the Internet (the Internet's network and communications) running while the latter are intended only for remote management by users, through the application of programs, algorithms and source codes designed by them.

In view of this, author also wants to articulate his opinion on defining boundaries of the interaction — in other words, criteria for categorizing "external" things involved in the interaction as things in the context of IoT. Should we include into the IoT things not only objects directly managed via the Internet (including vehicles and equipment) but also objects that are indirectly involved — the ones that are targeted by machines and equipment managed through the Internet? For instance, if a machine tool managed through the Internet processes a detail (not managed through the Internet), should one view this detail as a thing interacting in the IoT environment?

If one applies this broad approach — when all objects impacted by objects (machines and equipment) managed via the Internet are categorized as interacting things — it becomes difficult to establish clear boundaries for the category because such indirect impact would cover practically the entire material world — from traffic roads (which can be impacted, for instance, by transportation vehicles managed via the Internet) to foodstuffs (which, for instance, are quality controlled and packaged with an equipment managed as a thing in the IoT environment). In this writer's opinion, such approach is not helpful if we are to provide a clear idea of the phenomenon discussed here and formalize its essential features — in short, it is not helpful in the search for a pithy definition. Besides, this approach is at odds with several definitions of IoT, according to which a requisite feature of the managed thing is its electronic identification (see, for instance, the definition of IoT in the previously mentioned "Strategy for Developing an Information Society in the Russian Federation for 2017-2030"[38]) or the presence of the special technical devices embedded in the managed thing, such as detectors, sensors or actuators (see, for instance, the "Traffic Safety Concept for Public Roads with Driverless Transportation Vehicles"[39]).

It seems more accurate, therefore, to put in the category of interacting things only objects with the embedded technical devices or information

[38] Para 4("в") of the "Strategy for Developing an Information Society in the Russian Federation for 2017-2030," approved by Presidential Decree No. 203 of May 9, 2017.

[39] Section I of Traffic Safety Concept for Public Roads with Driverless Transportation Vehicles (DTVs)…

technologies enabling the system's software and technology complex to locate such objects and exchange electronic data with them (carry out electronic communication and information processing). And since the remote thing as such can interact electronically only when it is equipped with the special technical devices (embedded in the thing when it is manufactured or later), it seems justified to differentiate between the thing itself, which performs its user's commands, and the technical devices inside this thing, which transfer data (commands) from and to the thing and, therefore, warrant the categorization of this thing as the IoT thing.

It is also noteworthy that in addition to the term IoT, there are other terms that have currency — for instance, "the Internet thing" or "the Internet things," which certain authors refer to as "devices that can be connected to the Internet, usually via a Wi-Fi hotspot, and remotely managed, and autonomously perform their functions, receiving commands from the user essentially from anywhere in the world" [Gulyaev K.S., 2018: 29-37]. Some authors describe the Internet thing as "any device which, being connected to the Internet, can transfer or request certain data; has a particular address in the global web or an identifier enabling reception of feedback from the thing; and has an interface for interacting with the user" [Roslyakov A.V., Vanyashin S.V., Grebenkov A. Yu., 2015:10].

To avoid terminological confusion, the writer suggests that the Internet thing in the present context ought to be regarded simply as a separate thing within the general system of IoT (that is as "thing" in singular form in the term IoT); but when one needs to highlight the structural components or technical devices that keep the thing running in IoT, it appears justified to call them IoT's technical devices.

So, what is the character of things' interaction in IoT, can we identify any distinctive features of this interaction? In particular, may one argue that, in the given context, any exchange of electronic information among remote technical devices via the Internet is the sufficient condition for categorizing something as IoT — or such information exchange must have additional functionality-related (qualifying) distinguishing features?

As we see from the above definitions of IoT, some of them reference such interaction as an essential distinguishing feature of the concept, although the quality and character of such interaction is not always elaborated. In some definitions the explanation of communication among the Internet and remote objects contains the word "management" (management of things, of processes, etc.) — either in the description of the phenomenon

itself or in the elaboration of its function and purposes. Thus, some authors fairly point out that in the IoT environment physical objects (things), with embedded detectors and remote control and automatic management software, become connected automatically, without human intervention [Bratko A.G., Voluevich I.E., Glotov V.I. et al., 2018] and that IoT is capable of carrying out remote monitoring, control and management of processes in real time (including automatically) [Keshelava A.V., Budanov V.G., Rumyantsev V. Yu. et al., 2017: 8].

So, remote control and management are referenced as necessary distinguishing features of such interaction with/among remote things (via the Internet). The above mentioned "Recommended Practices for Introducing and Using the Industrial Internet of Things for Optimizing Control (Oversight)," too, highlight such distinguishing feature as control or management of things[40]. In other definitions, however, this aspect is not given due consideration, with the result that any electronic communications among remote objects (arguably including accidental or unauthorized interactions) can be called IoT; in this writer's opinion such understanding is at odds with IoT's definitions that include, as a vital feature, control over, or management of, things (see, for instance, the definition of IoT in the above mentioned annex to the Rosstat's order No. 463 of July 30, 2021).

Admitting that this question is open to debate, this writer believes however that a formulation of interaction of things that includes such characteristic as management or control is more accurate because management or control of things is the main purpose of IoT and it is the management/control function that is of economic, social and legal interest — this can be seen especially clearly in the above cited definitions of industrial IoT in laws and bylaws. So, it appears justified to include into a definition of IoT such function-related distinguishing feature as management of things, which characterizes interaction between the Internet and things or things among themselves. It follows from the above that not any electronic interaction of remote things should be considered as a distinguishing feature of IoT — only those interactions qualify whose purpose is remote management of things and which are carried out in the interest of the user or generated by an algorithm set by the user.

The next question to answer is what does "management of things" mean in the context of IoT.

[40] "Recommended Practices for Introducing and Using the Industrial Internet of Things " ...

Generally speaking, management is a purposeful and ongoing process — "a subject of management produces an impact on the object of management" [Popov L.L., Migachev Yu. I., Tikhomirov S.V., 2011]; the term "management," therefore, is very wide and applies to all possible types and methods of impacting objects for particular purposes — inter alia, the purpose of management in the legal sense, including transfer or other transactions. Similar legal interpretations of the term "management" are given in the Civil Code: Art. 37 and 38 (in the context of managing the ward's property), Art. 296 (in the context of operations management of the property of an organization or public enterprise), Art. 123.20-1 (in the context of managing the property of a fund), etc. So, in the context of IoT, should one limit the idea of management of things only to a physical or technological impact on the object of management (for instance, remote temperature check of a technological object, remote switching on/off of household or other appliances or processes, etc.) — or should one also include management in legal sense (for instance, agreements concluded or executed by the software and technology complex via the Internet)? Given that physical actions with the thing may be tantamount to an agreement or actions pursuant to an agreement (for instance, when a transportation vehicle managed via the Internet is transferred, with the use of remote commands, to a user, and delivered to the user without human intervention), such management may consist, inter alia, in concluding, or acting pursuant to, an agreement involving the thing. This writer believes that such an approach is not at odds either with the essence of management or with the essence of IoT (legal aspects of management of things are addressed in more detail in part 5 of the article).

Summing up the approaches to the substance of interaction among things in IoT, one would conclude that generally such interaction implies interaction between the Internet as a networked information and technology system, on the one hand, and remote objects, on the other, via the Internet's software and the technical devices embedded in these objects — an interaction for the purpose of managing such remote objects in the user's interest via electronic data exchange; management meanwhile can include both physical and legal actions with remote objects.

## 5. The place of IoT in law

IoT as a phenomenon is distinguished first of all by the new technological characteristic such as management of remote objects and processes. But

is IoT's role purely technical / technological? In particular, may one regard IoT as a legal phenomenon, as an object of law or a legal instrument?

IoT is already recognized as a legal phenomenon, which is evidenced at least by the inclusion of references to IoT in laws and bylaws (this issue has been studied in detail in part 3), so there can be no doubt on that score. One would imagine that this complex legal phenomenon quickly grow in scope, covering a wide spectrum of issues: from the consumer protection legislation (for example, in context of remote management of household appliances via IoT) to legislation on industrial and transportation safety (for example, in relation of the industrial IoT).

As for approaching IoT as an object of law, this question is more complicated since IoT is a complex phenomenon comprising many elements and aspects. One is led to believe that IoT, viewed as described above (that is as an infrastructural complex consisting of the information and technology system, software, and technological devices for remote management of distant objects), can hardly be considered as a single independent object of law by the current legislation. At the same time, separate elements of IoT (such as software, communication services, information, technical devices, etc.) can be objects of law regulated according to the general rules of civil law.

Although this approach is likely to generate controversy, this writer believes that in the area of contract law separate elements of IoT can be considered from at least three angles: as an element of the subject of a contract, as a method of performing obligations, and as an organizational and legal instrument or a legal environment (infrastructure, system) for concluding and performing agreements.

Thus, elements of IoT presumably can become a part of the subject of an agreement in case of a service agreement or a license agreement (for instance, an agreement on installation and technical support of a software-and-technology complex enabling remote management of objects) similar to agreements on software, communication services or Internet access.

On the other hand, IoT's technological system arguably can become a method to fulfill obligations if parties to an agreement agree to this (for instance, the use of IoT's technology for automatic remote relocation of distant objects, commanded by an algorithm or code agreed upon by the parties and programmed in the software).

And finally, yet another subject worth looking into is IoT's system as a legal infrastructure, as what might be called a "regulator" of transactions involving things (property). In particular, one can use IoT to regulate and

directly carry out economic legal transactions involving remotely managed things using Internet and software-and-technology tools which are sufficient for recognizing these transactions involving things as legitimate. What is meant by this is concluding agreements via the Internet, effecting transactions, sending commands (orders) related to remotely managed things, including, for instance, sending electronic commands from the technical device of the object or system managed in the interest of one user — to the technical device of the thing managed by another user (if algorithms of the interaction are designed to do so), and automatic acceptance of such commands according to the programmed terms. Or, in other words, using IoT to conclude and perform agreements generated by user-programmed algorithms in relation to remote objects (an example: managed remote things of one user electronically "order-request" to be relocated, so they are transported from one place to another, without human intervention, by another remote thing, and the transportation is carried out by an automatically managed transportation vehicle which is owned by another user and programmed to automatically accept such "orders-requests," when they meet certain criteria).

Such approach is close to the view of IoT as a crossbreed between a payment system, a registry of ownership rights in relation to things, and a system of concluding (formalizing, registering) agreements involving things. Thus, for instance, certain well known international payment systems already perform functions similar to the above with respect to certain property types (segments of interbank currency and lending markets) through electronic message exchanges in a formalized and protected information-and-technology infrastructure capable, inter alia, of recording rights and concluding and performing agreements (sure enough, the key difference is the absence of "things," in the classic sense, in the mentioned payment systems; given the context of our analysis, we take notice only of the similarity in the general principles of the systems' functioning). Federal Law No. 259-FZ meanwhile, regulating relations arising from the issue, recording and circulation of digital financial assets, clearly allows the issue, recording and circulation of digital rights in information systems (the information system is defined as an aggregation of information contained in databases and information technologies and technical devices for information processing, Art. 2 of Federal Law No.149-FZ) — in other words, highlights the eventual possibility of property (ownership rights) transactions in an information and technology system.

So, regulating procedures for concluding and performing agreements, as well as registering the rights to and, now, even effecting transactions with certain types of assets in the information and telecommunication networks and information systems — all these acts are already a reality, becoming regulated both at the level of agreements and, gradually, at the level of legislation (as it evolves). What is interesting in light of this is the fact, that the "Main Directions in the Development of Information Security in the Sphere of Credit and Finance for 2019-2021"[41] approach IoT precisely as an element of the payments sphere; what follows from this is that IoT, as was discussed above, can serve as a complex infrastructure for circulation of certain types of assets.

In view of the above, one would assume that if in such information-and-technology systems things are managed (remotely, by the user or the system programmed by the user) not only in the sense that they can be physically moved from one place to another, or that their technological functions or electronic communication capabilities can be put into play, but also in legal sense (by concluding agreements on handling such remotely managed things in line with the system's rules), then IoT presumably has an array of economic and legal functions that reaches beyond the strictly technological concept of IoT and, thus, requires an academic examination and legal analysis. And because of this IoT arguably may be called a complex organizational-technological and legal means (instrument) of concluding and performing agreements involving particular types of things which meet the requirements of the information and technology system (the software and technology complex) — in other words, IoT can be called an economic and legal infrastructure. Before these relations are exhaustively regulated by law, they may probably be regulated at corporate and contractual levels by parties involved (including, for instance, the use of smart contracts, discussed below). And if IoT also includes such element as management (administration) of things in legal sense, a possible consequence of this is commerce (trade) in them: then the question to answer, therefore, is how to differentiate between the concept and functions of IoT and the ideas of "electronic commerce" and "electronic trade."

Russia's federal laws have yet to provide definitions of the last two terms[42] while legal scholars debate their scope and relation to each other. The mod-

[41] Section "Background and Trends" // SPS Consultant Plus.

[42] These terms, however, are used in legislation in the broad sense of the word. For instance, "electronic trade" comes up in Order No. 279 of the Finance Ministry of December 21, 2018 "On Requirements to Appointed Postal Operators and on Procedures

el law "On Electronic Trade"[43] defines electronic trade as trade carried out with the use of information systems, the information and telecommunication network and electronic procedures; electronic procedures are defined as the manner of (rules of, procedure for) effecting electronic transactions pursuant to an agreement (Art. 2 of the Model Law). Some legal scholars already discussed such specific feature of electronic trade as effecting agreements via the information and telecommunication network [Andreeva L.V., 2019: 15–21]. Electronic commerce is sometimes considered the same as electronic trade, although in most cases the former term is defined more widely because it applies to a wide range of economic relations; for details see [Truntsevsky Yu. V., Ketsko K.V., 2020]. Thus, one of the widely accepted interpretations of electronic commerce is that it is "a totality of relations arising from entrepreneurial activities in the Internet — in particular, in the course of effecting agreements and/or promoting goods, works, services and other items via the Internet" [Saveliev A.I., 2016].

The idea of trade, or trading business, is defined in the legislation as a type of business activity involving acquisition and selling of goods (Art. 2 (1) of Federal Law No. 381-FZ of December 28, 2009 "On the Basics of State Regulation of Trade in the Russian Federation"[44]). In view of this, an appropriate definition for electronic trade arguably would be the activity involving acquisition and sale of goods, works, services with the use of an information and telecommunication network (in particular, the Internet).

So, from the economic and legal perspective, IoT, as an electronic information and technology system for concluding, recording and performing agreements involving remotely managed things, is close both to the concept of electronic trade, defined as trade with the use of the Internet, and the concept of electronic commerce, defined as a totality of relations arising from business activities in the Internet.

There is little doubt that IoT is a software and technology system first and foremost, whereas electronic commerce or electronic trade is a commercial activity in a wider sense; and the common factor in these two concepts is the environment of the activity — the use of the Internet as an information and telecommunication network (system). Sure enough,

for Paying Customs Duties, Taxes on Goods for Personal Use Acquired by Private Persons on an International Electronic Trade Platform and Sent to Buyers in International Mailings."

[43] Approved at the 31st plenary meeting of the CIS Interparliamentary Assembly, Order No. 31-12 of November 25, 2008.

[44] As amended April 4, 2022 // SPS Consultant Plus.

electronic commerce and electronic trade can be carried out without IoT's technologies and system, the same as IoT is far more than just a method or a form of carrying out electronic commerce — from the economic and legal perspective it has a wide range of capabilities in addition to trade: in particular, IoT can be used in any kinds of agreements, not just commercial or business agreements; moreover, it can be used in any electronic communications with managed things, and not just the ones bringing about legally important events (agreements).

Another interesting question is the relationship between IoT's functions and technologies, on the one hand, and the technology of distributed digital transaction ledgers (blockchain) connected together with the technology of smart contracts, on the other.

Analyzing these mutual relationships, author will use the definition of distributed ledgers provided in the already mentioned Federal Law No. 259-FZ: this is an aggregation of databases with replicated information, and the replication is ensured by programmed algorithms (Art.1 (7) of the Law). Scholars also use another definition of blockchain: a decentralized distributed database ("ledger") of all confirmed transactions effected in relation to a particular asset, and the functioning of this database is based on cryptographic algorithms. As one can see, both definitions are pivoted around the specifics of the algorithms ensuring the replication of the information, in other words — around the technology of processing (first of all recording, storing and protecting) information.

The legislation and regulations do not provide a definition of smart contract while legal scholars debate the meaning of the term. Not attempting to mention and analyze all definitions that have been proposed (this would require a separate study far beyond the scope of this article), let's focus on one of the widely used formulations: the smart contract is a contract in the form of a source code, implemented on the Blockchain platform and ensuring autonomy and self-performability of terms and conditions of such contract when circumstances stipulated in the contract are in place. That said, some scholars fairly note that "the smart contract, from legal viewpoint, can be regarded as an agreement in the form of a source code, whereas technologically the smart contract is like a source code" [Belitskaya A.V., Belykh V.S., Belyaeva O.A. et al., 2019]. Apparently, the smart contract is an array of distinguishing features comprising legal and informational-technological features, and this writer believes that the latter are essential for our understanding of the smart contract because they are what distin-

guishes the smart contract from ordinary agreements. In this context the smart contract appears to be a distinct complex technology for formalizing and mediating property transactions via the Internet, and this feature is similar to IoT's economic and legal functionality discussed above. The combination of the technologies of "smart contracts" (as a technology of concluding and performing agreements with the assistance of the Internet and a software) and "blockchain" (as a technology of recording the rights) creates a complex electronic infrastructure (system) that mediates property transactions both legally and technologically and, thanks to these characteristics, is close to IoT.

At the same time in view of author IoT has a wider range of functions: unlike the combined system of "smart contracts" and "blockchain," IoT, in addition to concluding and performing agreements, is also capable of direct management of remote objects (including the capability to physically move them or activate their certain functions) and of sending and receiving electronic communications to and from remote things themselves (to and from the technical devices in remote objects).

As for property transactions via the electronic system, the combination of "smart contract" and "blockchain" technologies is not the only possible option, nor is it inseparably linked to IoT: as discussed earlier in the article, similar acts of concluding, registering, recording and performing agreements via informational-technological systems can be carried out, on the one hand, with the use of IoT and without the "smart contract" and "blockchain" technologies, and on the other, without the use of IoT altogether.

Because of it, the reviewed functions and technologies of IoT, as well as of "smart contracts" and "blockchain," should arguably be evaluated as independent phenomena or instruments. One can envisage, however, situations when these technologies are used synchronously (jointly): the conclusion and performance of agreements in an IoT environment can also involve the use of the "smart contract" and "blockchain" technologies, which, however, can function outside IoT as well (for instance, in an intranet, a specialized corporate or other local network).

So, positioning of IoT in law arguably should be based on IoT's legal definition reflecting the its legal substance, its key distinguishing features as a legal phenomenon. Since a legal definition of IoT is still in the making, the argument about IoT's place in law (from the three main angles) advanced here is not uncontroversial. At the same time there is little doubt that IoT is bound to become seriously regulated — this is necessary both

for protecting interests of parties involved (contractors, consumers, etc.) and for promoting business activities in this sphere (from developing and selling software to construction and transportation), which is especially important for industrial IoT.

## 6. Searching for a complex definition of IoT

On the whole, the definition of IoT probably should reflect logical interconnections of the terms used ("the Internet" and "thing") and have the form of a generalization combining the features of both. The substance of each of the terms was discussed above, but it is also important to understand the logical connection between them when they are brought together in one phrase.

So, IoT arguably should be approached as a phenomenon rooted in one of the practical applications of the Internet in conjunction with the additional elements — the software and the special technical devices of managed things (that matter was addressed in parts 3 and 4 above).

Next, if we are to produce an accurate formulation of "things" in the context of IoT taking into consideration the different approaches discussed in part 2), we need to correctly define the term "things" in relation to IoT and, generally, evaluate the appropriateness of using it in this context.

At first thought, if the phenomenon discussed here is about managing remote objects, then perhaps it would be best to call it "the Internet of objects"? At the same time, objects are usually understood as material phenomena [Ozhegov S.I., 2018: 470], although in some documents (including, inter alia, the above mentioned ISO Standards) immaterial objects are included in the category of things. Some of the scholarly treatments discussed above, too, take a broader view of "things" in the context of IoT, including in it immaterial objects, "virtual things" and other similar types of immaterial assets in the widest sense — probably even such objects are not even recognized as property at all by Russian law. So, there is an obvious incongruity between the legal understanding of "things" and the not infrequent common understanding of IoT.

Thanks to its technology, IoT in principle can be applied to objects which are, strictly speaking, not things or objects: for instance, the function of remote management can be applied, inter alia, to certain informational elements (source codes or databases; or information in electronic form contained in electronic registries or computer software in general), which

are called in some texts "virtual objects" (if the technical devices of IoT are adapted accordingly). Besides, IoT's technological base can be also used instrumentally for managing ownership rights (for instance, in payment infrastructures or rights recording systems, discussed above). Under this broader interpretive approach, it is necessary to find a different appellation for managed entities because, for obvious reasons, the notion of "thing" in legal sense is inaccurate in this context. Not all interpretations of IoT, however, are based on this broad approach: for instance, the definition of IoT in the "Traffic Safety Concept for Public Roads with Driverless Transportation Vehicles (DTVs)," mentioned above, includes in IoT sensors and actuators, which are material objects. The mentioned sensors and actuators, therefore, may be likewise applied only to material objects indicating material, rather than virtual, nature of managed things. IoT in this context apparently covers only things in the classic sense. Such situation makes it more difficult to arrive at a general concept that would encompass both the narrow and the wide approaches in the context of a satisfactory description of managed objects (things): in the narrow sense, IoT is for managing material objects, whereas in the broad sense, it is for managing a broader range of items, including immaterial (virtual) ones.

Evaluating, in general, attempts to find proper terminology for situations when the word "thing" is used to describe immaterial items, one is lead to conclude that the proper choice would be terms whose substance and scope correspond to the substance and scope of their definitions in legislation currently in force. When an idea is transplanted to the sphere of law and one gives it meanings and readings different from the ones prevailing in this sphere, this runs contrary to the rules of legal workmanship, makes an obstacle to clear understanding of legal norms and proper application of law, and can cause ambiguity and practical disagreements. It appears necessary, therefore, to use terms in line with their established legal meaning (understanding) when attempting to explain (elaborate) concepts. But if the scope and character of a phenomenon defined does not correspond with the established definition of legal terms selected for description of such phenomenon, then the proper course of action arguably would be not to adapt the understanding of particular terms to suit particular cases but to find different, more accurate concepts best suited to the relevant features and the essence of the phenomenon defined.

So, if an analysis of the term used to explain the new phenomenon shows that the meaning de-facto given to the term "thing" applied in this new context is not in line with the established legal understanding of the term,

one should arguably look for another term, the one best suited to reflect the specific substance of the idea (phenomenon), rather than impart to the term "thing" a legally unorthodox meaning in this specific context. So, for description of the concepts of the entire group of virtual informational elements, in this writer's opinion, the term "objects" appears more appropriate than "things" because the term "object" may encompass both material and immaterial elements and, so, is best suited for capturing the entire range of possible manifestations of the phenomenon under review.

In view of the above, there is another question that may arise — would it not be more appropriate to speak about management of property (property being a broader idea than things) and, in particular, about "the Internet of property" since this term covers both things and other types of property? In author's opinion, however, this approach will hardly make understanding easier because law does not always catch up with the pace of information technologies and private commerce, so the result can be that parties to transactions will be taking interest in new entities that are not yet regulated by law (not yet recognized as property) but already function as objects of the parties' actions (for instance, so called "virtual things"). Besides, in case of transborder dealings via the Internet, such approach may cause conflicts between parties' national laws (because what one legal system recognizes as property may be not regarded as such by another). Considering this, one would advise to choose more universal but also broader term for describing objects managed in the IoT environment.

So, in author's opinion, "object" in the given context is a more accurate term:

it is already used in law for describing the most diverse types of property[45], which shows that its use is an acceptable and well-established legal technique in similar situations,

it is used when one needs to come up with the pithiest definition encompassing all possible interests of parties to transactions (including in the context of objects of civil-law transactions, Art. 128 of the Civil Code), and this allows to capture a fairly wide part of the phenomenon discussed, without creating a conflict with other legal categories.

[45] See, for instance, Art.130 (1) of the Civil Code of the RF, in relation to the description of immovable property, or the Protocol on Guarding and Protecting Intellectual Property Rights (Annex 26 to the Treaty on the Eurasian Economic Union of May 29, 2014), about the description of results of intellectual activity, or Art. 38 (1) of the Tax Code of the RF, for the description of taxable items.

So, in author's opinion, producing a universal (broad) description of IoT, it is arguably more appropriate to use the term "objects," and it is appropriate in relation both to the definition and the term itself. "The Internet of objects" therefore appears to be a more accurate definition for what is now called IoT. Let's note that this term also comes up in specialized literature: for instance, authors of certain professional texts admit that IoT is sometimes called "the Internet of objects." [46]

Next, identifying elements and distinguishing features necessary for defining IoT, this writer will take into account the following. One would argue that only those distinguishing features of IoT qualify for inclusion into the definition are always present in IoT, across the entire range of areas of activity where IoT is applied. From methodological perspective, it is inappropriate to widen or narrow the term IoT depending on one of its practical applications or on one of IoT's possible technologies of recording or processing data — there is a clear need for a single universal unambiguous definition, applicable to any of the manifestations of the essence, and/or any application, of IoT — such definition ought to include only basic, fundamental properties, without which IoT cannot function. So, variable elements related to particular technologies, which can change because of progress in science and technology or fluctuations in market trends, should be left out.

And what elements of IoT are indispensable? As demonstrated above, they arguably include the following:

Internet as an information and technology system of communication and transfer and receipt (processing) of information (the basic information-and-technology platform of IoT);

additional software-and-technology complex as a software solution for connecting to and communicating with remote entities;

remote objects connected to the first two elements with the assistance of the software and the technical devices of the objects themselves — in other words, objects whose software and technology is compatible with the system's;

function-related distinguishing feature of the entire system of elements listed above — remote management of the object in the user's interests thanks to the system's electronic (wireless) communication with this object.

[46] See, for instance, CISCO's presentation. Available at: URL: https://www.cisco.com/c/dam/global/ru_ru/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf (accessed: 28.04.2022)

At the core of the described phenomenon, meanwhile, is arguably management or, more specifically, management of remote entities (objects) with the assistance of the special technical devices and technologies (the Internet, software, the technical devices of managed objects) — and it is for the purpose of management that the entire system is created and functions. The definitions emphasizing only communication among things or the technical infrastructure, in this writer's opinion, do not embrace all of the system's core elements: in particular, they leave out either the phenomenon's function-related distinguishing features or the user's will (and users unavoidably participate in management — by installing reproducible algorithms or software, or by sending one-off electronic messages expressing their will — sending commands to the software-and-technology complex or to remote entities' technical devices capable of receiving, processing and transferring data in electronic format). The abstract electronic "communication among things" per se is obviously too amorphous a formulation to convey a holistic idea of the phenomenon; besides, what also seems quite certain is that things as such cannot "communicate" among themselves as they wish because they are not capable of expressing a will nor do they possess any modicum of reason. The same applies to their interaction, of course if we mean by it managed interaction, rather than physical interaction activated by physical forces of nature (for instance, gravity). Any "interaction" of remote objects with the system or among themselves, therefore, is an instance of execution, by these objects' software and/or technical devices, of algorithms or settings that were designed by the user via the system that enables electronic data exchange; and, so, the user's participation in management of remote entities must be reflected in the description of the phenomenon discussed.

A correct understanding of the process, therefore, requires that one should take a broader analytical approach, embracing an array of the elements and distinguishing features related to the "interacting things": the software (information and technology complex), the subject of the expression of the will, the purposes, the means, the mechanisms of management. But relying on the previously formulated idea of the Internet as a system, one would think that it is reasonable and logically and methodologically consistent to also understand IoT as a system, and given the previously discussed main functional purpose of the system, to understand it as a system of management before all.

So, approaching these elements and distinguishing features as one system and integrating substantive (indispensable) features and elements into

a single conceptual framework, you come up with approximately the following extensive definition of IoT: it is a software and technology system of remote management of remote objects carried out in the user's interest with the assistance of the Internet and the managed objects' technical devices capable of electronic data exchange. That definition emphasizes not communication itself or its technical infrastructure but the substantive aspect — management of remote objects in the user's interest with the assistance of the software connected to the Internet and the technical devices (capabilities) of the remote object itself. Such conceptual emphasis arguably allows, first, to better reflect the phenomenon's essence, functions and intended purpose, and second, to translate the concept into a language that is more familiar to practitioners of law. And substituting "things" with "objects," we eliminate the possible incongruity with the classic interpretation of things in Russian law.

Actually, explaining various phenomena and processes related thereto through the phrase "management system" is a technique not infrequently used for describing similar phenomena based on the concept of interconnections among various distributed elements that are of interest to the user in the context of influencing them by intervening (managing). It is this logic (the logic of management systems) that underpins such concepts of the Russian law as, for instance, risk management system (Art. 28 of Federal Law No.161-FZ of June 27, 2011 "On National Payment System"[47]), industrial security management system (Art. 9 of Federal Law No.116-FZ of July 21, 1997 "On Industrial Safety at Hazardous Industrial Facilities"[48]), and, closer to the context discussed here, property management system (for instance, Part III of the federal special-purpose program "Developing a Single State System of Rights Registration and Land Registry (2014–2020)"[49], as well as para 1 of the Governmental Order no. 841 (June 29, 2019)[50].

[47] Revised July 2, 2021 with changes and updates in force since December 1, 2021.

[48] Revised June 11, 2021.

[49] Approved by the Governmental Order No. 903 of October 10, 2013 (revised April 22, 2020) "On the Federal Purpose-Oriented Program 'Development of an Integrated State System of Ownership Rights Registration and Cadastral Registration of Immovable Assets (2014-2020)."

[50] Governmental Order No. 841 of June 29, 2019 "On Organizing Ring-Fenced Accounting of Property Created and/or Acquired as a Result of the Realization of Programs, Subprograms, Projects and Activities of the CIS, and On Introducing Amendments to the Regulations on the Federal Agency for Managing State Property" (together with the "Rules on Filling Out Maps of Accounting Items Located in the Russian Federation and Created and/or Acquired in the Course of Realization of a Program, Subprogram, Project or Activity of the Commonwealth of Independent States").

So, the phrase "management system" — "system of management" of objects (including, for instance, property) is arguably an established phrase used in law for describing similar phenomena or processes; this writer believes it is justified to use it in the present context as well. In this case all technical and technological ("infrastructural") characteristics of the described phenomenon can probably be viewed as properties and distinguishing features of this system. As discussed above, they include first of all the use of the Internet as a means of communication and a technological environment, as well as the use of the additional software and technical devices enabling electronic data exchanges with managed entities (objects).

Sure, understanding what constitutes the essence of IoT is still largely in progress; deliberators meanwhile have pointed out certain controversial issues and questions that require, inter alia, a discussion from the perspective of legal scholarship. And sure enough, the proposed approach to understanding IoT will require further elaboration, clarification and fine-tuning: there can be little doubt that further development of the legislation and the publication of new studies addressing these issues will help identify and take into account new factors or manifestations of the phenomenon under review.

Considering that the Internet technologies and the terminology related thereto continue to develop, at a pace that not only does not show signs of slowing down but gains momentum as scientific progress advances, there is a continuous need for timely scholarly analysis of the quickly changing terminology. So, there can be little doubt that IoT needs further in-depth analysis and a universal definition. In particular, some authors argue that the main problem to grapple with in the foreseeable future would be harmonizing various standards in order to form a single and consistent regulatory framework for practical use of IoT.

Some researchers fairly argue that we need to develop an open-ended concept outlining legal aspects of IoT in the Russian legal system and possible vectors of their regulation [Arkhipov V.V., Naumov V.B., Pchelintsev G.A., Chirko Ya. A., 2016].

Considering the vital relevance of these questions and the transborder character of the Internet relations, one would suggest organizing international conferences and round tables of legal scholars devoted to problems and prospects of legal regulation of IoT. Author also believes, that relevant proposals should be developed by national academic task groups comprising legal scholars and information technology experts.

Author hopes that the approaches and legal positions presented in the article would promote additional research into, and discussions among legal scholars about, the subject.

## References

1. Andreyeva L.V. (2019) Elements of Digital Technologies in Commerce and Procurement. *Predprinimatelskoe pravo*=Enrepreneurship Legislation, no. 1, supplement, pp. 15–21 (in Russ.)

2. Anisimova A.A., Bevzenko R.S., Belov V.A. et al. (2018) Clause-by-Clause Commentary on the Russian Legislation on Notaries. Moscow: Statute, 719 p. (in Russ.)

3. Arkhipov V.V. (2020). The Internet Legislation: Theory and Hands-On Training Guide for Institutions of Higher Learning. Moscow: Yurist, 249 p. (in Russ.)

4. Arkhipov V.V., Naumov V.B., Pchelintsev G.A., Chirko Ya.A. (2016) Open-ended Concept of Regulating the Internet of Things. *Informatisonnoe pravo*=Information Law, no. 2, pp. 18-25 (in Russ.)

5. Bagoyan Ye. G. (2019) Information Security and the Use of the Blockchain Technology: International Experience and the Need for Legal Regulation in Russia. *Yurist*=Lawyer, no. 3, pp. 42–49 (in Russ.)

6. Belitskaya A.V., Belykh V.S., Belyaeva O.A. et al. (2019) Legal Regulation of Economic Relations at the Present Stage of Digital Economy. M.A. Egorova (ed.). Moscow: Yustitsinformv, 376 p. (in Russ.)

7. Bratko A.G., Voluevich I. Ye., Glotov V.I. et al. (2018) Financial Monitoring: Reference Book for Undergraduate and Graduate Students. Moscow: Yustitsinform, 480 p. (in Russ.)

8. Danilenkov A.V. (2014) *The Internet Law*. Moscow: Yustitsinform, 232 p. (in Russ.)

9. Fedotov M.A. et al. (2019) Information Law: Textbook for Undergraduate, Specialist Degree and Graduate Students. Moscow: Yurist, 497 p. (in Russ.)

10. Gillis A. (2021) What is Internet of things. Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (accessed: 09.04.2021)

11. Gulyaev K.S. (2018) A Person's Right of Access to the Internet, Rights in the Internet Environment, and Rights in the Internet of Things Environment: New Trends. *Pretsedenty Yevropeyskogo suda po pravam cheloveka*=Case Law of the European Court of Human Rights, no. 1, pp. 29–37 (in Russ.)

12. Illarionova T.I., Kirillova M. Ya. et al. (1985) Soviet Civil Law: Study Guide. Moscow: Vysshaya shkola, 544 p. (in Russ.)

13. Iliyn V.D., Kharabet K.V. (2016) The Internet. In: The Great Russian Encyclopedia. Available at: URL: https://bigenc.ru/technology_and_technique/text/2014701#litra (accessed: 14.04.2021) (in Russ.)

14. Jackson L. (2016) Internet of Things Bill Introduced. *National Law Review*, vol. 6, p. 69.

15. Keshelava A.V., Budanov V.G., Rumyantsev V. Yu. et al. (2017) Digital Economy. On Threshold of Digital Future. Available at: URL: http://sp-kurdyumov.ru/uploads/2017/07/vvedenie-v-cifrovuyu-ekonomiku-na-poroge-cifrovogo-budushhego.pdf. (accessed: 11.05.2022) (in Russ.)

16. Kopylov V.A. (2002) Information Law: Textbook. Moscow: Yurist, 512 p. (in Russ.)

17. Kozhemyakin D.V. (2019) *Domain Names As Applied to Objects of Civil-Law Rights*. Moscow: Prospect, 152 p. (in Russ.)

18. Kozlov S.V. (2016) Legal Regulation of Relations in the Internet, or What Does the Internet Law Mean. *Pravo i ekonomika*=Law and Economy, no. 11, pp. 26–29 (in Russ.)

19. Lovtsov D.A. (2011) Information Law: Textbook. Moscow: RAP, 228 p. (in Russ.)

20. Morgan J. (2014) Simple Explanation of Internet of Things. Available at: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=441defc81d09 (accessed: 09.04.2022)

21. Naumov V.B. (2018) Negative Aspects of the Formation of the Conceptual Framework in the Area of Regulation of the Internet and Identification. *Informatcionnoe pravo*=Information Law, no. 1, pp. 32–39 (in Russ.)

22. Popov L.L., Migachev Yu. I., Tikhomirov S.V. (2011) *State Management and the Executive Branch: Substance and Balance*. Moscow: Norma, 320 p. (in Russ.)

23. Rassolov I.M. (2009) *Law and the Internet. Theoretical Problems.* 2nd ed. Moscow: Norma, 383 p. (in Russ.)

24. Roslyakov A.V., Vanyashin S.V., Grebeshkov A. Yu. (2015) The Internet of Things: A Learning Guide. Samara: PGUTI Press, 200 p. (in Russ.)

25. Rustambekov I.R. (2015) On the Legal Concept of the Internet. *Informatsionnoe pravo*=Information Law, no. 3, pp. 22–26 (in Russ.)

26. Saveliev A.I. (2016) Contract Law 2.0: “Smart” Contracts as the Beginning of the End of the Classic Contract Law. *Vestnik grazhdanskogo prava*=Civil Law Courier, no. 3, pp. 32–60 (in Russ.)

27. Sazhenov A.V. (2018) Cryptocurrencies: Dematerialization of the Category of Things in Civil Law. *Zakon*=Law, no. 9, pp. 106–121 (in Russ.)

28. Sinitsyn S.A. (2016) The Thing as an Object of Civil-Law Rights: Possible and Necessary Criteria for Identification. *Zakonodatel'stvo i ekonomika*=Legislation and Economy, no. 11, pp. 7–17 (in Russ.)

29. Sklovsky K.I., Kostko V.S. (2018) On the Idea of Thing. Money. Immovable Property. *Vestnik ekonomicheskogo pravosudia*=Courier of Business Justice, no. 7, pp. 115–143 (in Russ.)

30. Sukhanov Ye. A. (2017) Right In Rem: a Scholarly and Educational Essay. Moscow: Statute, 560 p. (in Russ.)

31. Truntsevsky Yu. V., Ketsko K.V. (2020) Criminal Risks of Electronic Commerce: International and National Aspects. *Mezhdunarodnoe publichnoe i chastnoe pravo*=International Public and Private Law, no. 6, pp. 18–22 (in Russ.)

**Information about the author:**

B.Yu. Dorofeev — Candidate of Sciences (Law), Associate Professor.

The article was submitted to editorial office 18.02.2021; approved after reviewing 12.05.2021; accepted for publication 10.09.2021.

Law in the Digital Age. 2022. Vol. 3. No 2.
Вопросы права в цифровую эпоху. 2022. Т. 3. № 2.

*Research article*
JEL: K33
DOI:10.17323/2713-2749.2022.2.49.72

# The Legal Status of Crypto-Asset Issuers in the Light of the Proposed MICA Regulation

**Yana Daudrikh**
Faculty of Law, Comenius University, 6 Safarikovo namestie, Bratislava 810000, Slovak Republic. E-mail: yana.daudrikh@flaw.uniba.sk

**Abstract**

The progress of modern digital technologies raises the question on the necessity of common regulatory mechanism applicable to crypto-asset issuers and embracing comprehensive regulation of the status of all parties involved in crypto-asset trade. However, regulation of major parties provided by the V. AML Directive has been inconsistent and abstract.[1] Under pressure of policy-makers and professional community, the European Commission has come up with the long awaited draft MICA regulation[2] designed to ensure universal regulation of crypto-assets across all member states of the European Union (hereafter EU) including those of the European Economic Area (hereafter EEA). The proposed draft purports to harmonize fragmented regulation of crypto-assets which EU member states were forced to introduce for lack of EU-wise regulation of this institution. The main purpose of this paper is to analyze the newly established institutions including categorization of crypto-assets covered by MICA. The main functional aspects of the crypto-asset offering process including a requirement to publish a white paper are examined in this context. The supervisory role of the European Banking Authority (EBA) in respect of the issuers of significant crypto-assets is specifically discussed. Based on this analysis, the author concludes

[1] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

[2] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. COM/2021/420 final.