ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

2/2022

Volume 3

Legal Issues in the **DIGITAL AGE**

Publisher
National Research
University Higher
School of Economics

2/2022

ISSUED QUARTERLY VOLUME 3

Articles

Comment

Book Review

Legal Issues in the **DIGITAL AGE**

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

"Legal Issues in the Digital Age" Journal is an academic quarterly e-publication which provides a comprehensive analysis of law in the digital world. The Journal is international in scope, and its primary objective is to address the legal issues of the continually evolving nature of digital technological advances and the necessarily immediate responses to such developments.

The Digital Age represents an era of Information Technology and Information Communication Technology which is creating a reliable infrastructure to the society, taking the nations towards higher level through, efficient production and communication using digital data. But the digital world exposes loopholes in the current law and calls for legal solutions.

"Legal Issues in the Digital Age" Journal is dedicated to providing a platform for the development of novel and analytical thinking among, academics and legal practitioners. The Journal encourages the discussions on the topics of interdisciplinary nature, and it includes the intersection of law, technology, industry and policies involved in the field around the world.

"Legal Issues in the Digital Age" is a highly professional, double-blind refereed journal and an authoritative source of information in the field of IT, ICT, Cyber related policy and law.

Authors are invited to submit papers covering their state-of-the-art research addressing regulation issues in the digital environment. The editors encourage theoretical and comparative approaches, as well as accounts from the legal perspectives of different countries.

The journal is registered in the Federal Service of Supervision of Communications, Information Technology and Mass Media. Certification of registration of mass media серия Эл № ФС77-83367

ISSN 2713-2749

Address: 3 Bolshoy Triohsviatitelsky Per.,
Moscow 109028, Russia
Tel.: +7 (495) 220-99-87
https://digitalawjournal.hse.ru/
e-mail: lawjournal@hse.ru

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.

that the application of MICA is handicapped by a number of problems discussed in more detail further on. Thus, MICA is not straightforward in its definitions of crypto-assets which are rather general, and contains no detailed explanation of cooperation between the competent authorities in the EU and third countries to prevent money laundering and terrorist financing. The following research methods were used by the author in writing the paper: formal legal method, comparison, synthesis, analysis, analogy, induction and deduction methods.

Keywords

MICA; crypto-asset; money laundering and terrorist financing; utility token; asset-referenced token; e-money token; white paper; supervision of token issuers.

For citation: Daudrikh Y. (2022) The Legal Status of Crypto-Asset Issuers in the Light of the Proposed MICA Regulation. *Legal Issues in the Digital Age*, vol. 3, no. 2, pp. 49–72. DOI:10.17323/2713-2749.2022.2.49.72

Background

On 7 May 2020, the European Commission put forward an action plan for creation of comprehensive European Union policy to prevent money laundering and terrorist financing.[3] Under the proposed plan, the European Commission was to take steps for tighter EU regulation against money laundering and terrorist financing. This was followed by four legislative proposals regarded as a single agreed package and designed to implement the EC's action plan. The package contains four proposals[4] which completely change the effective law to introduce an EU-wide code for preventing unauthorized use of the financial system for money laundering and terrorist financing.

[3] Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing. COM (2020) 2800 final.

[4] 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. Proposal for a Directive of the European parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, COM/2021/423 final. Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, COM/2021/421 final. Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast), COM/2021/422 final.

On 24 September 2020 the European Commission presented under the proposed plan a new Digital Finance Strategy with a focus on four main areas: overcoming fragmentation of the single digital market; adapting the EU regulatory framework to promote digital innovations; advancing data-based finance; addressing problems and risks of the digital transformation including to improve digital transactions and ensure sustainability of the financial system.[5]

The Digital Finance Strategy is largely based on the proposed MICA regulation whereby the European Commission intends to bring the EU regulatory framework in line with the FATF (Financial Action Task Force) recommendations which, in particular, define the key concepts (for instance, crypto-assets, crypto-asset service provider etc.).[6] With the EU intending to back financial sector innovations, MICA strives to support the activities of crypto-asset issuers while underlining the need to protect consumers. Thus, MICA does not concern itself with developing measures to restrict the use of crypto-assets within the EU.

As part of MICA, the European Commission introduces an individualized legal regime to remove the risks posed by crypto-assets and significant tokens.[7] Due to the similar legal nature of crypto-assets, securities and e-money, MICA includes certain provisions of the MIFID[8] and the e-money directives[9] [Hobza M., 2021: 19].

Despite that the Digital Finance Strategy is a landmark in terms of encouraging innovations and promoting digitization, MICA's definitive form is up-to-date unclear and raises a number of sufficient questions regard-

[5] Communication form the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions on a Digital Finance Strategy for the EU, COM(2020) 591 final.

[6] FATF Report. Virtual Currencies Key Definitions and Potential AML/CFT Risks. Paris: FATF, 2014; see akso: FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Interpretive note to recommendation 15 (new technologies). Paris: FATF, 2012.

[7] Explanatory memorandum to proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final, p. 8.

[8] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

[9] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

ing its relevance and formal adequacy. The ambiguity and inconsistency of MICA's legal form are noticeable throughout its content.

1. The scope of MICA

The draft of MICA regulations applies to the offering of crypto-assets and provision of related services in the EU[10] meaning that MICA largely covers the territory of the EU. However, the draft of MICA regulation is also important for the EEA and its relevant provisions are thus equally applicable to EEA member states [Ferreira A., Sandner P., Dünser T., 2021: 23].

Since crypto-asset offering is a rather broad area, there are certain exemptions from the proposed MICA regulation for the most part related to operations subject to other regulations (for example, MIFID, e-money and deposit guarantee schemes directives[11] etc.). Digital currencies of central banks are equally exempt provided that these are crypto-assets issued by central banks in the capacity of a monetary authority. Other exemptions include, for instance, the European Investment Bank, insurance companies, public international organizations etc.[12]

Currently, the EU adopts the technological neutrality principle[13] whereby the issuer may choose the technology to use, with a majority of crypto-assets relying on the distributed ledger technology ("DLT"). As the V. AML directive, apart from this requirement, provides no explanation of this concept, we have to turn to the eIDAS directive[14] where the technological neutrality is understood as the absence of requirement to use specific national technology for electronic identification in a particular EU member state.

[10] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 2 (1).

[11] Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes Text with EEA relevance.

[12] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937. COM (2020) 593 final. Art 2 (3).

[13] 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. Recital 22.

[14] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Art 12 (3) (a).

In the DLT context, MICA applies the term "distributed ledger technology" which means the one supporting distributed data encryption.[15] The DLT facilitates digital identification [Zetzsche D., Arner D., Buckley R., Weber R., 2020: 334]. In this case, it should be underlined that most DLT technologies will relate user accounts not to their real identification data but to an account ID functioning as an alias [Moreno S., Seigneur J., Gotzev G., 2020: 9]. DLT is characterized by totally or almost decentralized management and fully decentralized record keeping [Zetzsche D., Arner D., Buckley R., 2020: 180, 334].

2. Types of crypto-assets

Compared to the original, currently effective V. AML regulation, MICA offers a totally different classification of crypto-assets divided into a number of specific types of tokens.

The original term "virtual currency" defined in paragraph 18, Article 3 of V. AML thus gives place to the general term "crypto-assets". Compared to the former, the latter is a much broader term which, apart from digitally representing a value, represents to some extent the rights related to ownership of crypto-assets.

Based on the definition of crypto-assets, the following three sub-categories of tokens are distinguished:

utility token ("UT");

asset-referenced token ("ART");

e-money token ("EMT").

MICA envisages the emergence of new technologies in the future and therefore gives the European Commission broader powers to be able, as necessary, to adopt delegated acts for amending the original definitions of the terms in line with the market development and technological change.[16] This competence allows MICA to be flexible in responding to future innovations and changes to the core elements of adaptable concepts.

2.1. Utility token

While not normally regarded a traditional form of security or financial product, UT is a crypto-asset type which provides digital access to a com-

[15] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM (2020) 593 final. Art 3 (1).

[16] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM(2020) 593 final. Art 2 (2).

modity or service available via DLT, with their acceptance linked to the given token's issuer.[17] UTs serve non-financial purposes primarily related to the use of digital platforms and digital services. Thus, UTs are designed to support the functionality of blockchain-based systems rather than generate future cash flows [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 206].

UTs can also provide a means of exchange which, unlike ARTs or EMTs, is not linked to any asset. One example is bitcoin which is not linked to any legal tender or other type of commodity [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 212 — 213]; [Irwin A., Turner A., 2018: 299]. It is obviously bitcoin that is targeted by Chapter II of the MICA regulation.

While Chapter II entitled "Crypto-assets other than asset-referenced tokens or e-money tokens" makes no reference to UTs ("other crypto-assets"), it is this chapter that regulates UTs [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 211]. The use of a different term ("crypto-assets other than asset-referenced tokens or e-money tokens") probably reflects an attempt to embrace all currently existing and future types of tokens not detailed in the proposed MICA regulation.

The provisions of Chapter II contain general regulation of UT trading. Primarily targeting issuers of "other crypto-assets", these provisions introduce a number of eligibility requirements to issuers wishing to offer the said crypto-assets to the public or seeking their admission to a trading platform in the EU.

One of the requirements concerns the status of crypto-asset issuers which should be established as a legal entity. In fact, each issuer trading in crypto currencies through a platform should be a legal entity. Apart from this general requirement, no form of incorporation or reference to a draft or amendment to the relevant EU legislation is mentioned. Theoretically, it means the issuer can be established as a limited liability company. While we cannot judge what was the legislator's original intention, we believe it would be feasible, in order to reduce a higher risk involved in crypto currency trade, to opt for the joint-stock company as a form envisaging tighter requirements, in particular, to capital since this would finally ensure better protection of crypto-assets held by consumers.

Issuers of other crypto-assets are basically supervised by competent authorities of their home EU member state meaning the member state where they have their registered address as a legal entity. It is the competent au-

[17] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM(2020) 593 final. Art 3 (1) (5).

thority of the home EU member state that is required to notify the white paper to the European Securities and Markets Authority ("ESMA"). The ESMA will provide public access to the white paper in the register of crypto-asset service providers.[18]

The proposed MICA resolution adopts a specific approach to the question of the issuer offering "other crypto-assets" to the public or seeking their admission to a trading platform. In this case, the territorial principle is applied, with the home EU member state advising the host EU member state of the issuer's intention.[19] The host EU member state is the one in whose territory the issuer is about to offer its crypto-assets.

In the context of these conclusions, it becomes obvious that the issuers of "other crypto-assets" are supervised at the level of EU member states which raises the question of cooperation with third countries. As the relevant MICA provisions do not address this question in detail, we take the recital as the starting point which says that the issuers established in a third country should notify their white paper to the competent authority of the EU member state where the crypto-assets are to be offered or where the admission to trading on a trading platform for crypto-assets is sought in the first place.[20]

2.1.1. White paper

One of the main requirements to issuers of other crypto-assets concerns the drafting, notification and publication of a "white paper". The content of the latter is detailed in paragraph 1, Article 5 of the MICA regulation.

The rules to draft and publish "white paper" are not principally different from those of a prospectus. Moreover, the fact that the implementation powers specified in Chapter II are assumed by the ESMA makes the similarities between the "white paper" and the prospectus even more striking [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 211].

In fact, the proposed MICA regulation contains a number of statements advising consumers of the risks involved, so that they are not mislead with regard to the legal classification of crypto currencies. For instance, MICA

[18] For details of the register of crypto-asset service providers see: Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM(2020) 593 final. Art 57.

[19] Ibid. Art 7 (4).

[20] Ibid. Recital 18.

requires to notify the consumers that the "white paper" was not reviewed or approved by any competent authority in any EU member state.[21] At the same time, the issuer is required to state that the white paper is not a prospectus and that crypto-assets are not regarded as financial instruments.

In this regard, the "white paper" should not contain any assertions on the future value of crypto-assets, unless the issuer of such "other crypto-assets" can explicitly guarantee their future value.[22]

In fact, it is the risk involved in crypto-asset trading that has forced to introduce additional responsibility of the issuer of "other crypto-assets" for the information contained in the "white paper". If the information is incomplete, false or misleading, the issuer will compensate for the damage caused to the crypto-asset holder. The issuer's liability allows no exclusion.[23] In this case, there is no liberal reason (such as force-majeure circumstances) which would waive the issuer's liability for the caused damage. Thus, once the crypto-asset holder provides evidence of violation of the provisions, the issuer will be liable to compensate for the damage. However, it is worth noting that the issuer's absolute liability does not apply to the summary deemed to be part of the "white paper".[24] In this case, the legislator does not allow to claim damages caused by the information contained therein.

With reference to the EU's original intent to support innovations in the financial sector, the MICA regulation contains a list of exclusions in paragraph 2, Article 4 which exempt crypto-asset issuers from the requirement to draft, notify or publish a "white paper". In doing this, the legislator obviously wished to reduce the burden on smaller issuers trading in such crypto-assets. Some of the exclusions reflect the core principle of proportionality to stress that the proposed rules should be limited to what is required to achieve the draft's purpose.[25]

The principle of proportionality also applies to MICA provisions on no ex ante approval of a "white paper" to be sought from the competent authority of the home EU member state [Bočánek M., 2021: 43]. At the same time, issuers are required to notify the "white paper"'s content to the

[21] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM(2020) 593 final. Art. 5 (3).

[22] Ibid. Art. 5 (4).

[23] Ibid. Art. 14.

[24] Ibid. Art. 22 (3).

[25] Explanatory memorandum to proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM(2020) 593 final, p. 5.

competent authority of the home member state 20 business days before the publication date. The notification must explain to the competent authority why the offered crypto-asset is qualified as such (and not as some other financial instrument).[26]

Since there is no ex ante approval of the "white paper", the question is whether the proposed regulation is feasible. The argument to avoid overload on the competent authorities is inherently weak in view of the high risks involved. It is theoretically possible that a person interested in crypto-assets may be given different versions of the "white paper", for example, due to a sudden partial change of its content, only to make the purchase of such crypto-assets more problematic. Therefore, we believe it is feasible to revisit the issue of ex ante approval by the competent authority to ensure adequate integrity and certainty through EU-wide regulation [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 212].

2.2. Asset-referenced token

ARTs are defined as "a type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets".[27] In this case, tokens linked to a basket of currencies, commodity types or crypto-assets are meant [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 212]. The stable value of such tokens allows holders to use them as a legal tender for purchase of goods and services or for saving.

To offer such tokens or apply for admission of such assets to a trading platform, the ART issuer must have an authorization issued by the competent authority of the home EU member state. The authorization should be issued by the EU member state where the issuer has a registered address as a legal entity. The content of an application for authorization is detailed in Article 16, one of the main requirements being the white paper submitted to the competent authority for approval.

The issued authorization is subject to the principle of single European passport otherwise called passporting. This principle means that the autho-

[26] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM(2020) 593 final. Art 7 (1–3).

[27] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 3 (3).

rization will take effect in the territory of all EU member states [Winkler M., 2004: 705]. Also, the passporting principle applies to the content of the proposed "white paper".

This is a major change, with the currently effective voluntary registration giving place to mandatory registration. Compared to V. AML[28] which did not explicitly require issuers to obtain authorization for the given type of business, the new regulation represents a higher level of harmonization to introduce a single access point to the financial market. However, it should be stressed that in spite of these advantages, the authorization is likely to be more cumbersome to obtain for smaller token issuers.

The proposed MICA regulation also contains a number of exclusions from the authorization requirement. Thus, no authorization is required for issuers holding a banking license[29], offering tokens exclusively to qualified investors etc.[30] However the fact of not being obliged to seek authorization does not waive the ART issuer's obligation to publish a "white paper".

The process of authorization can be divided into two stages:

applying for authorization;

making a decision to issue or deny authorization.

At the first stage, the competent authority of the home EU member state will check the submitted application and its necessary annexes for completeness. Then the competent authority will assess the ART issuer's compliance with the effective requirements over three months to make a well-founded draft decision to issue or deny the sought authorization.

At the second stage, the competent authority will provide their draft decision to issue or deny authorization including requests for opinion addressed to the EBA, ESMA and ECB (European Central Bank), with the said agencies to propose their non-binding opinion to the competent authority within two months. The competent authority will make the final decision to issue or deny authorization based on this opinion. Where the

[28] 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. Recital 9.

[29] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC. Art 8.

[30] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 15 (3–4).

ART issuer's application has been satisfied, the authorization will be added to the register of crypto-asset service providers maintained by the ESMA.

The competent authority may withdraw the authorization where the issuer no longer complies with any of the requirements envisaged by paragraph 1, Article 20 of the MICA regulation — for instance, if the issuer no longer complies with all of the qualification requirements etc.

The authorization process is explicitly linked to ART issuers' obligation to draft and publish a "white paper". Under paragraph 1, Article 17 of the MICA regulation, ART issuers, unlike issuers of "other crypto-assets", while not required to advise consumers of review and approval of the "white paper" by the competent authority of their home EU member state, have to describe, among other things, their reserve of assets. The "white paper" is deemed automatically approved if the issuer has received the authorization for public offering of ARTs or admission to the trading platform. In this context, ART issuers have to seek the approval of their white paper by the competent authority of the home EU member state.

The requirement to seek the approval of a white paper has been added to ensure the protection of consumers and market integrity from higher risk associated with ARTs compared to "other crypto-assets" which follows from their possibly broader use (for instance, as a legal tender).

As in the case of "other crypto-assets", the information on future value cannot be part of a white paper. Also, ARTs come under certain exclusions envisaged by paragraph 2, Article 4 of the MICA regulation which exempt ART issuers from the requirement to draft and publish a "white paper".

2.2.1. Governance arrangements and capital requirements

ART issuers should have robust governance arrangements including a clear organizational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which they are or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures.

There is a special requirement applicable to members of the management body of ART issuers. In the first place, they should have good repute, competence and experience. At the same time, the said members should provide evidence that they were not convicted of offences relating to money laundering or terrorist financing or other financial crimes. There require-

ments also apply to natural persons holding a qualified stake in the ART issuer or otherwise exercising a power of control over such issuer.[31]

In order to reduce the existing risks, ART issuers should have internal control arrangements as well as risk assessment and management procedures. This implies the use of RBA (risk-based approach) based on FATF Recommendations.[32]

In order to offer crypto-assets, ART issuers should have in place own funds of EUR 350,000 or 2% of the average amount of the reserve assets calculated as of the end of each calendar month over a prior six-month period.[33]

Apart from the obligation to have in place own funds, ART issuers are required to have and maintain reserve of assets. Reserve assets are a group of currencies which are legal tenders, exchange traded commodities or crypto-assets underlying the value of ARTs and available for investment. If several ART categories have been issued, the average amount of the reserve assets should be maintained in respect of each category.

The EU member state hosting the ART issuer may decide to increase/decrease the said percentage requirement to the average amount of the reserve assets by maximum 20% depending on the assessment of specific facts indicating a higher or lower risk. These facts may assume, for example, the quality and volatility of the reserve assets or the aggregate value and number of transactions carried out in ARTs.[34] This raises the question: whether a higher percentage requirement will not prevent smaller players from accessing the market. The proposed burden may prove to be cost-prohibitive to them.

Issuers are required to keep a reserve of assets separately from own funds. Based on a contract concluded in advance, the issuer should keep the reserve assets in custody with a crypto-asset service provider or a credit institution. The choice of a custodian will depend on the type of the reserve assets to be kept in custody. While credit institutions accept fiat currencies, financial instruments and other assets, crypto-asset service provides will not keep in custody anything other than crypto-assets.

[31] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 30 (2–4).

[32] FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Interpretive note to recommendation 15 (New technologies). Paris, FATF, 2012, p. 10.

[33] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 31 (1).

[34] Ibid. Art 31 (3).

Credit institutions and crypto-asset service providers are liable for possible loss of financial instruments or crypto-assets placed in their custody and will be obliged to return to ART issuers a financial instrument or a crypto-asset of an identical type or the corresponding value. To waive this liability, the legislator envisaged a classical liberal basis whereby a credit institution or a crypto-asset service provider may prove that the loss has resulted from an external event beyond their reasonable control, the consequences of which would have been unavoidable despite all reasonable efforts.[35]

Pursuant to Article 34 of the MICA regulation, ART issuers may invest a part of their reserve assets in highly liquid financial instruments. Such investments should be capable of being liquidated rapidly, with all losses and risks involved to be borne by ART issuers.

ART issuers are prohibited from paying interest throughout the term in which consumers are in possession of such tokens.

2.3. E-money token

The EMT means a type of crypto-asset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender.[36] Thanks to this broad concept, the legislator has covered a majority of crypto-asset types compatible with the above requirements.[37]

Compared to ARTs, EMTs are primarily designed to be a legal tender for the purchase of goods and services, with a stable value to be maintained through a link to only one fiat currency.[38]

Issuers of such tokens should comply with the three main requirements:[39]

be authorized as a credit institution or an electronic money institution;

comply with requirements applying to electronic money institution;

publish a white paper.

---

[35] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 33 (8).

[36] Ibid. Art 3 (4).

[37] Národná banka Slovenska. Prehľad trhu s kryptoaktívami v Slovenskej republike. November 2020, p. 6.

[38] Ibid. P. 5.

[39] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 43 (1).

Unlike ARTs, no specific authorization is required in this case. Thus, the EMT offering is based on the existing regulation of credit institutions and on regulation of electronic money institutions.

The term credit institution means a company operating to accept deposits and other refundable monetary funds from the population as well as to issue credit at its own expense.[40] An example of credit institutions is a bank.

An electronic money institution is a legal entity authorized to issue e-money on the basis of compliance with specific requirements.[41] While e-money[42] is not conceptually identical to EMTs, the latter was associated with e-money to apply this concept[43] [Sidak M., Slezáková A., 2014: 105].

Authorization depends on compliance with the established requirements to be regulated in more detail by specific provisions. In case of a credit institution, the list of requirements depends on regulation applicable in specific member states.[44] This rule also applies to electronic money institutions which should comply with the requirements detailed in the relevant national law of the specific EU member state.[45]

Like in the case of ARTs, MICA contains a number of exclusions regarding authorization of EMT issuers. Thus, EMT issuers are exempt from authorization if e-money tokens are offered exclusively to qualified inves-

[40] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012. Art 4 (1).

[41] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. Art 2 (1).

[42] Pursuant to Art 2 (2), Directive 2009 mentioned, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, e-money is a monetary value maintained in electronic form (including magnetic records) which constitutes the issuer's obligation to accept money to perform payment transactions as defined by Art 4 (5), Directive 2007/64/EC and which is accepted by other natural persons or legal entities different from the issuer of e-money.

[43] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 43 (1).

[44] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC. Art 8 (1).

[45] For instance, the Slovak Republic applies para 82, Law No. 492/2009 Z. z. on payment services and amendments to specific laws (zakon č. 492/2009 Z. z. "O platobných službách a o zmene a doplnení niektorých zákonov").

tors or their amount does not exceed EUR 5,000,000 over a period of 12 months.[46]

Apart from compliance with the said requirements, issuers should also comply with other requirements detailed in Chapters II and III of the e-money directive.

In contrast to ARTs, there is no requirement to have in place and keep in custody any reserve assets.

Moreover, pursuant to Article 49 EMT issuers may invest the funds received in exchange for EMTs in secure, low-risk assets denominated in the same currency as the one referenced by the e-money token. The list of such secure, low-risk assets is regulated by paragraph 2, Article 7 of the e-money directive with reference to annex I of the voided directive on capital adequacy of investment firms and credit institutions[47]. The legislator will obviously need to remove the reference to voided directives and replace them with those to effective regulations.

EMT issuers are prohibited from paying interest throughout the term in which consumers are in possession of such tokens, a requirement reflecting Article 12 of the e-money directive. The prohibition to pay interest is designed to make sure EMTs are used as a legal tender rather than a value saving instrument. In other words, it is an attempt to separate tokens from securities covered by a different regulatory domain [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 216].

ART issuers are also required to publish "white paper" by notifying the relevant authority of their home EU member state in advance. Like in the case of issuers of other crypto-assets, the EMT "white paper" is not subject to ex ante approval by the competent authority of the home EU member state.

3. The EBA supervisory objectives in respect of significant token issuers

3.1. Significant tokens

The EBA will supervise the issuers of significant ARTs and EMTs.

The EBA will classify ARTs as significant depending on whether issuers meet at least three main criteria. A more detailed list of criteria is provided

[46] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 43 (2).

[47] Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions.

in paragraph 1, Article 39 of the MICA regulation — for instance, the size of the issuer's reserve assets, the value of the tokens issued etc. In this case, the proposed regulation has only a general list of criteria without specifying them in detail. Further detailing of these criteria will be provided by delegated acts which the European Commission is authorized to issue.

The EBA's decision will depend on whether the issuer meets the above criteria as reported by the competent authority of the home EU member state. Based on the analysis of information provided, the EBA will or will not classify the given ART as significant. The EBA will then issue a draft decision to be notified to the ART issuer and the competent authority of the EU member state, with the supervisory function to be delegated to the EBA in cooperation with the relevant authority of the home EU member state. In this case, supervision of significant tokens will be exercised exclusively by the EBA.

Under the proposed MICA regulation, ART issuers may wish to classify their tokens as significant. In this case, they should demonstrate, through a programme of operations including the applicable business model, that the tokens meet at least three of the required criteria. Based on the provided information, the EBA will or will not classify such tokens as significant.[48] In light of the above it is obvious that if the EBA does not classify a token as significant, the issuer will continue to be supervised by the home EU member state.

Apart from general requirements, the issuers of significant tokens are required to meet additional requirements which, unlike those of ART issuers,[49] mainly differ in that the average amount of the reserve assets is increased from original 2% to 3%.[50]

As in the case of ARTs, EMT issuers are required to meet at least three criteria detailed in Article 39 of the MICA regulation.

The process whereby the EBA will classify EMTs as significant is similar to that applying to ARTs.

The main differences from ARTs manifest themselves in the following. In the first case, we deal with voluntary classification of tokens as significant. To apply for such classification, issuers need to be authorized as a banking institution or an electronic money institution.

[48] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 40.

[49] See part 2.1 of this paper for more detail on the main requirements to issuers.

[50] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 41 (1).

Another difference is that the list of additional requirements applicable to EMT issuers has been changed. For instance, EMT issuers are required to have in place and hold in custody the reserve assets capable of being invested,[51] with the requirement of 3% of their average amount to be observed in this case. [52]

In view of a broader use of significant EMTs as a legal tender and the risks they may pose to sustainability of the financial system, it was necessary to double the supervision over EMT issuers, to be ensured jointly by the competent authority of the home EU member state and the EBA.

3.2. Consultative college

Once a decision is made to classify tokens as significant, the EBA will establish a "consultative college" for each issuer of such tokens. The college will consist of a number of agencies (for instance, EBA, ESMA, ECB, competent authority of the EU member state) as well as the competent authorities of the most relevant crypto-asset service providers etc.[53] However, there is no definition of the most relevant entity in the proposed MICA regulation. In this context, paragraph 6, Article 99, and Article 101 underline the need in draft regulatory standards to be developed by the EBA in cooperation with ESMA and the European System of Central Banks to specify the conditions under which such entities are to be considered as the most relevant.

The core objectives of the college are:

issue opinions to be used as supporting materials to the proposed draft white paper etc;[54]

exchange information;[55]

agree on delegation of the main tasks to college members.[56]

The EBA will also charge a fee to reimburse a competent authority for costs incurred as a result of supervision of significant token issuers. The

[51] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 33 and 34.

[52] Ibid. Art 52.

[53] Ibid. Art 99 (2) and 101 (2).

[54] Ibid. Art 100 (1) and 102 (1).

[55] Ibid. Art 107.

[56] Ibid. Art 120.

amount of the fee charged on ART issuers should be established pro rata to the amount of their reserve assets while that charged on EMT issuers pro rata to the amount of their outstanding e-money.

3.3. Powers of the EBA in respect of significant token issuers

To supervise the issuers of significant token, the EBA has the power to perform inspections, for instance, by summoning the issuers to provide explanations, orally or in writing, on the subject of review, or to check whether issuers comply with all requirements established by relevant regulations etc.

The EBA has the power of on-site inspection at all offices of issuers, as may be necessary, to be performed on the basis of a relevant decision adopted by the EBA. The decision should specify the subject, reason and date of inspection as well as sanction in the form of a penalty for refusal to cooperate with the EBA. The amount of penalty will depend on the extent of violation of the applicable MICA provisions [Winkler M., 2018: 290].

The EBA is required to notify the inspection to the competent authority of the EU member state where the issuer holds its registered address. For adequate and efficient control, the EBA may perform on-site inspection without prior advice to the issuer.

On-site inspection should be performed by officers or other persons authorized by the EBA on the basis of a permission in writing. Should the issuer oppose to on-site inspection, a competent authority of the home EU member state should render the necessary assistance to the officers or ask the police for help.

The legality of decisions made by the EBA can be verified only by the European Court of Justice.[57] Courts at EU member states have the right to request the EBA to provide information on suspected infringement of the MICA regulation including on the status of suspects.

The EBA may apply administrative sanctions to issuers for infringement of MICA, with the form of administrative liability detailed in Annexes V and VI. The EBA may simultaneously apply one or more forms of administrative sanctions.

[57] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC. Art 61.

The forms of applicable administrative sanctions depends on the type of tokens. The range of administrative liability envisaged by the legislator in respect of ARTs is rather broad compared to EMTs where a narrower list of possible sanctions is specified. Thus, the EBA may prohibit an issuer of significant ARTs from offering such tokens, withdraw its authorization etc. In the case of EMT issuers, the EBA may apply a penalty to a significant token issuer for a failure to comply with all requirements.[58]

4. Practical problems related to the implementation of MICA

The draft MICA resolution will put in place novel and at the same time broad regulation of crypto currency trade. In this context, we note a number of practical problems which are likely to arise in the course of its implementation.

Classification of crypto-assets. Overall, the classification of crypto-assets proposed in MICA would cover a majority of the existing tokens. However, hybrid tokens combining the features of several tokens might be difficult to classify. In this case, each EU member state may have its own classification of such tokens — for instance, as financial instruments, e-money or exchange traded commodities [Burilov V., 2019: 164–165]. At the same time, it will be necessary to identify whether a given crypto-asset falls within the scope of the MIFID or e-money directive. In this case, there is a doubt whether specific directives rightly apply to hybrid tokens. [Blandin A., Cloots A. Et al., 2019: 18]; [Ferrari V., 2020: 329].

Broad definitions of tokens. The legislator's attempt to cover a broad range of specific crypto-asset types with specific notions has equally resulted in a practical problem, only to make it difficult to apply the proposed notions to hybrid tokens.

Another matter of concern is the change regarding the notion of UTs. Once introduced by paragraph 5, Article 3, it is no longer used in other provisions which adopt instead a new term — particularly, other crypto-assets — not defined anywhere in the text. Judging from the professional literature, one would suppose other crypto-assets will be an equivalent of UTs [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 211].

[58] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 112 (1–2).

It should be underlined in this regard that pursuant to paragraph 2, Article 3 the legislator empowers the European Commission to adopt delegated acts to specify technical elements of specific types of crypto-assets. The European Commission may thus amend the original definitions of token types with the purpose of improving and adapting them to the evolving crypto-asset market and technological change. At the first glance, this MICA provision is fairly reasonable and future-focused but, on the other hand, we cannot but endorse the opinion on the existence of practical problems in this domain.

Since there are currently more than 8,000 types of crypto-assets in the world, it would be obviously hard to deal with all their specific features at a time. The amended notions should be, on the one hand, fairly broad and abstract to cover these different types and, on the other hand, accurate, so as to close loopholes for possible infringement of law. Where the existing definitions are amended or extended, it will be also necessary to amend or expand the range of powers of the regulatory authorities in EU member states. In view of the above, we deal with the problem related to the length of the legislative process and the willingness of EU institutions to amend the already effective and time-tested legal acts [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 220–221].

Authorization and approval of a "white paper". While the issuers of ARTs and EMTs should be authorized to offer their tokens, no such authorization is required for UTs. A similar approach applies to drafting and publication of a white paper where UT issuers are not required to seek authorization of the competent authority while ART and EMT issuers are. This approach can finally aggravate the risk of the issuer going back on its original decision to offer ARTs and EMTs precisely because of this regulatory burden including a stricter form of supervision by competent authorities of EU member states.

Drafting/publication of a "white paper". There is inconsistent regulation as regards exemptions for smaller issuers. In the case of other crypto-assets, the proposed regulation exempts issuers from drafting/publishing a white paper provided that the total outstanding crypto-assets offered in the EU over one year do not exceed EUR 1,000,000 or the offered crypto-assets can only be held by qualified investors.[59]

This exclusion also applies to ART and EMT issuers which do not need an authorization to do business. The exclusions will apply to small issuers,

[59] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. Art 4 (2).

once the average outstanding amount of tokens over a period of 12 months calculated at the end of each calendar day does not exceed EUR 5,000,000 or once ARTs are offered exclusively to qualified investors.[60]

A comparison of the exclusions mentioned above makes it obvious that ART and EMT issuers are not exempted from the requirement to draft and publish a "white paper". Thus, even small issuers for whom no authorization is required must draft and publish a "white paper". This interpretation will introduce, to say the least, unfair regulation concerning the drafting of a white paper, and pose the question of whether such regulation is appropriate [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 222 — 223].

Cooperation with third countries. MICA covers exclusively the territory of the EU and EEA. Since crypto-asset trade is not limited to the territory of the EU [Houben R., Snyers A., 2018: 11], the question is whether this is appropriate. Cooperation with third countries is only mentioned in Article 90 which authorizes competent authorities of the EU member states to conclude cooperation arrangements with supervisory authorities of third countries concerning the exchange of information and the enforcement of obligations arising under the MICA regulation in third countries. The role of the EBA and ESMA is to coordinate the development of such arrangements. As such, the ESMA is expected to draft technical regulatory standards containing a template document for cooperation arrangements. In our opinion, this is a complicated and rather cumbersome method of establishing cooperation, unless the core aspects of the content of such arrangements are specified in the first place.

Another question concerns the position of third countries as members of the Consultative College to be established by the EBA for issuers of significant tokens. The College members can include relevant supervisory authorities of third countries, once the EBA has concluded administrative agreements with them under Article 108 of the MICA regulation. The College members from EU member states have the right to vote for or against a joint decision of the College while supervisory authorities of third countries don't. In this case, it is not quite clear why the legislator, in proposing membership to supervisory authorities of third countries, did not give the voting right at the same time. Obviously, the decisions to be passed by the College will not be enforced by third countries despite the membership [Ferreira A., Sandner P., Dünser T., 2021: 1].

[60] Ibid. Art 15 (3) (a) and 43 (2) (b).

Decentralized issuance of crypto-assets. A fundamental problem related to MICA's application is decentralized issuance of crypto-assets where issuers are not identified in the first place [Zetzsche D., Arner D., Buckley R., Annunziata F., 2021: 224]; [Hornuf L., Kück T., Schwienbacher A., 2021: 13]. It is expected that each issuer will disclose its identity in the interest of transacting in crypto-assets and will meet all requirements established by the MICA regulation at the same time. Obviously, the decentralized issuance of crypto-assets will pose a serious and currently unsolvable problem of finding a way to force such issuers to seek authorization and submit themselves to the supervision of competent authorities.

Conclusion

Inadequate regulation of crypto-assets still observed in the EU has been a cause of shadow environment for crypto-asset business which has not yet been subject to strict control. The proposed MICA regulation is expected to fill the existing gap in this area, in the first place through unification of new institutions, such as ARTs or significant tokens. There is obvious progress, particularly regarding perception of specific tokens which have been so far understood under the V. AML directive as a kind of virtual currency exchangeable for fiat currencies or other types of virtual currencies.

The draft MICA resolution can be considered one of the most ambitious projects in the EU. At the same time, it cannot be neglected that MICA is a combination of already effective and time-tested regulations closely related with crypto-asset trade. In this regard, it is similar to MIFID and e-money directive whose provisions were partially borrowed word for word or partially amended and adapted to the process of crypto-asset trade.

Based on the above analysis, it can be concluded that, once applied in its current form, MICA is likely to raise criticism on the part of both EU member states and professional community. In terms of application, the main problems concern the classification of tokens which is inadequate and likely to apply to all categories of crypto-assets in the future. The authorization requirement applicable to ART and EMT issuers also raises the question of possible evasion of law and choosing UTs as an easier option. Obtaining a banking license is fairly cumbersome for a credit institution wishing to issue only ARTs and EMTs. As an extra benefit, UTs do not require to seek the approval of a white paper and are much easier to deal with as UT issuers are not subject to strict control and additional requirements. While we understand the legislator's attempt to tighten the regulation of ARTs

and EMTs as coming into direct contact with the EU's real economy, we disagree with a totally different form of regulation and higher regulatory burden on ART/EMT issuers. This stance could eventually slow down the development and innovation in digital technologies — precisely as a result of the excessive burden on those interested in crypto-asset trade. The problem of non-exemption of small ART and EMT issuers from the requirement to publish a white paper is manifested in a similar way, only to stress the difficulty of meeting the established requirements compared to UTs.

Last but not least, there is inadequate regulation of the cooperation with third countries restricted to possible cooperation arrangements to be concluded between competent authorities of EU member states and such third countries. In view of the global scope of crypto-asset trade, this method of cooperation appears especially deficient. There is an obvious need to raise the question of deeper cooperation at the level of the EU institutions. Therefore, we believe it necessary to establish a common and specific procedure for cooperation with third countries whereby the latter would have the same rights as the respective EU member states.

References

1. Blandin A., Cloots A. et al. (2019) *Global Cryptoasset Regulatory Landscape Study*. Cambridge: University Press, 122 p.

2. Bočánek M. (2021) First Draft of Crypto-Asset Regulation (MiCA) with the European Union and Potential Implementation. *Financial Law Review*, issue 22, pp. 37–53.

3. Burilov V. (2019) Regulation of Crypto Tokens and Initial Coin Offerings in the EU de lege lata and de lege ferenda. *European Journal of Comparative Law and Governance*, vol. 6, pp. 146–186.

4. Ferrari V. (2020) The regulation of crypto-assets in the EU — investment and payment tokens under the radar. *Maastricht Journal of European and Comparative Law*, vol. 27, pp. 325–342.

5. Ferreira A., Sandner P., Dünser T. (2021) Cryptocurrencies, DLT and crypto assets: the road to regulatory recognition in Europe. Available at: https://ssrn.com/abstract=3891401 (accessed: 09.10.2021)

6. Hobza M. (2021) Challenges of Law in Business and Finance. 13th International Scholar Conference "Law in Business of Selected Member States of the European Union". Prague: TROYAS, pp. 13–22.

7. Hornuf L., Kück T., Schwienbacher A. (2021) Initial coin offerings, information disclosure, and fraud. CESifo Working Paper No. 7962. Germany: Munich Society for the Promotion of Economic Research — CESifo GmbH, pp. 1–46.

8. Houben R., Snyers A. (2018) Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion. Brussels: European Parliament, Policy Department for Economic, Research and Quality of Life Policies, 101 p.

9. Irwin A., Turner A. (2018) Illicit Bitcoin transactions: challenges in getting to who, what, when and where. *Journal of Money Laundering Control*, vol. 21, no. 3, pp. 297–313.

10. Moreno S., Seigneur J., Gotzev G. (2020) Handbook of Research on Cyber Crime and Information Privacy. Hershey: Information Science Reference, 400 p.

11. Sidak M., Slezáková A. (2014) Regulácia a dohľad nad činnosťou subjektov finančného trhu. Bratislava: Wolters Kluwer, 238 p. (in Slovak)

12. Winkler M. (2004) Legal aspects of conducting business by Slovak banks within the common market of the EU (on the example of the Czech Republic). Business Entrepreneurship and Marketing in the New European Economic Area: Almanac of an International Conference on the Occasion of the 35th Anniversary of the Faculty of Business held under the auspices of Ivan Miklos, Deputy Prime Minister of the Slovak Republic. Bratislava: EKONÓM, pp. 703–710.

13. Winkler M. (2018) Regulation of deadlines for issuing decisions in proceedings conducted pursuant to the Financial Market Supervision Act. Law governing conducting business in selected member states of the European Union. International Conference. Law governing conducting business in selected member states of the European Union. Almanac of the 10th International Scholar Conference. Prague: TROYAS, pp. 277–284.

14. Zetzsche D., Arner D., Buckley R. (2020) Decentralized Finance. *Journal of Financial Regulation*, vol. 6, issue 2, pp. 172–203.

15. Zetzsche D., Arner D., Buckley R. (2020) The evolution and future of data-driven finance in the EU. Common Market Law Review, vol. 57, issue 2, pp. 331–360.

16. Zetzsche D., Arner D., Buckley R., Annunziata F. (2021) The Markets in Crypto-Assets regulation and the EU digital finance strategy. *Capital Markets Law Journal*, vol. 16, issue 2, pp. 203–225.

Information about the author:

Y. Daudrikh — Assistant Professor, PhD, JUDr. (Slovak Republic), Leading Researcher.

The article was submitted to the editorial office 24.10.2021; approved after reviewing 12.01.2022; accepted for publication 30.01.2022.

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

Research article
УДК: К 33, К 36
DOI:10.17323/2713-2749.2022.2.73.89

Privacy of a Child in the Digital Environment: New Risks Unaddressed

Natalya Vyatcheslavovna Kravchuk

Institute of Scientific Information for Social Sciences of the Russian Academy of Sciences, 15 Krzhizhanovskogo Str., Moscow 117218, Russia, natkravchuk@mail.ru

Abstract

Digital technologies have brought with them new possibilities for exercising and protecting human rights; however, their potential for violations of human rights has also grown exponentially. Use of ICT influences the daily lives of adults, but their impact on children is even greater, as the risks of harm they face are now mediated and exacerbated online. The importance of children's right to privacy has manifested itself anew in the context of digital technologies. In addition to concerns about safety, there are other considerations such as data processing and the "digital footprints" created by children themselves. Parents have traditionally been considered the primary agents for guidance and support of children's rights online as well as for the protection of their children, but they are now seen as their children's main publicity agents. Nevertheless, the problem of "sharenting" remains unaddressed at both the national and international levels. Measures developed to protect the privacy of the child follow a paradigm of rendering support to parents without stressing their obligation not to disclose information about their child. The General Comment on children's rights in relation to the digital environment adopted by the UN Committee on the Rights of the Child in 2021 reflects this approach. Its stance demonstrates the power of traditional perceptions that reinforce seeing the child as an object incontestably cared for and ruled by their parents This precludes consideration of parents' online activities as potentially harmful to their children and also impedes the development of norms and remedies for protecting the right of the child to privacy against infringements by their parents.

Keywords

human rights; rights of the child; right to privacy; digital environment; parents; sharenting; UN Committee on the Rights of the Child.

For citation: Kravchuk N.V. (2022) Privacy of a Child in the Digital Environment: New Risks Unaddressed. *Legal Issues in the Digital Age*, vol. 3, no. 2. pp. 73–89. DOI:10.17323/2713-2749.2022.2.73.89

Introduction

The relationships between the digital environment[1] and human rights are complex ones. These relationships have attracted the attention of scholars and policymakers as well as international organizations. A body of norms for protecting human rights, including the right for privacy, from ICT-specific risks or risks elevated by digital technologies is being formulated at the international level.

The importance of the right of a child for privacy has manifested itself anew in the digital environment. The risk factors faced by children and that are being addressed include safety, data processing and "digital footprints" created by children themselves. Parents play a key role in guiding and supporting the exercise of children's rights online, as well as ensuring their safety. Accordingly, the measures developed to protect the privacy of the child are being framed within the paradigm of rendering support to parents.

The problem of "sharenting" — use of social media to share news, images, etc. of one's children — remains unaddressed at both the national and international levels even though this phenomenon and the risks it poses to children's privacy have been the object of numerous academic studies. In this article it is argued that, as the United Nations General Comment on children's rights in relation to the digital environment demonstrates, the international community is not yet ready to move away from the basic premise that parents should be supported in their role as a child's representative and defender but should not otherwise be controlled. This precludes

[1] "Digital environment" is understood as encompassing information and communication technologies (ICT), including the internet, mobile and associated technologies and devices, as well as digital networks, databases, content and services (Recommendation CM/Rec (2018)7 of the Committee of Ministers of the Council of Europe to Member States on guidelines to respect, protect and fulfill the rights of a child in the digital environment).

consideration of parents' online activities as potentially harmful to their children and also hampers development of norms and remedies aimed at defense of the right of the child to privacy against infringements by their parents both on international fora and within national jurisdictions.

The remainder of this paper is divided into five sections. Section 1 outlines the developments in the international legislative accommodation of interactions between the digital environment and human rights. Section 2 explores global and regional responses to the risks to children's rights mediated and exacerbated on the Internet. Section 3 analyses various contexts in which the privacy of the child is addressed. Section 4 characterizes the recently recognized phenomenon of sharenting. Section 5 explores national and international efforts to regulate sharenting.

1. Human rights and the digital environment

An analysis of the interactions between the digital environment and human rights requires an understanding of the specific nature of this environment. Researcher M.L. Trajkovska, among many, notes new technologies are characterized by their global character, the swift dissemination of information, and the endless possibilities of the replication of that information. These technologies have brought with them new possibilities for exercising and protecting human rights. However, the possibilities for violating human rights have also grown exponentially [Trajkovska M.L., 2015: 335].

Adaptation of both national and international rules to advances in science and technology is frequently perceived as being too slow and consequently inadequate for regulating new legal situations created by developments in ICT and its influence on social culture. Making those rules more responsive to ICT requires a reconceptualization of traditional human rights in light of the latest technological developments [Coccoli J., 2017: 224]. This process is being conducted at the global and regional levels simultaneously.

The Resolution "The Right for Privacy in the Digital Age", adopted in 2013 by the UN General Assembly, has stressed that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy as set out in Article

12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights; and that right is therefore an issue of increasing concern.[2] The right to privacy was consequently considered not only as one of the rights most affected by digitalization, but also as a gateway to the realization of human rights.

After a number of preliminary studies, consultations, and the introduction of the mandate for the Special Rapporteur on the right to privacy a report under the title "The Right to Privacy in the Digital Age" was issued by the United Nations High Commissioner for Human Rights.[3] Although a variety of measures had been introduced at the regional level to protect human rights, including the European Union's General Data Protection Regulation; the Council of Europe's Protocol to update and modernize the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the African Union Commission's Personal Data Protection Guidelines for Africa, the UN High Commissioners report emphasized that many laws or items of proposed legislation in this regard fall short of applicable international human rights standards and raise serious concerns (para. 2 of the Report). The High Commissioner has recommended that national governments recognize the full range of implications that new technologies have for the right to privacy but also for all other human rights; that they adopt strong, robust and comprehensive privacy legislation that complies with international human rights law in terms of safeguards, oversight and remedies to effectively protect the right to privacy; that they establish independent authorities with powers to monitor state and private sector data privacy practices, investigate abuses, receive complaints from individuals and organizations, and issue fines and other effective penalties for the unlawful processing of personal data by private and public bodies; and that they ensure that all victims of violations and abuses of the right to privacy have access to effective remedies (para. 61 of the Report).

At the regional level the "living instrument" doctrine developed by the European Court of Human Rights (hereinafter ECtHR) provides premises that are ideally suited for adjusting the obligations of the state to meet today's challenges to human rights. The idea that the European Convention on Human Rights (hereinafter ECHR) must arrive at positions that are aligned with present-day conditions and that evolve through the interpre-

[2] A/RES/68/167 of 18 December 2013.

[3] A/HRC/39/29 of 3 August 2018.

tation of the Court has been a central feature of ECtHR case law from its early days. The ECHR has shown that it is capable of evolving in parallel with society. In this respect its formulations have proved their worth over several decades [Wildhaber L., 2004: 84]. During the last several years the ECtHR lived up to this doctrine when it considered a number of cases covering issues such as the use and protection of electronic data, use of email, GPS, the Internet, surveillance and radio communications.[4] In particular, the Court emphasized the importance of a prudent approach to a state's positive obligations to protect human rights in new environments and of the need to recognize the diversity of possible methods to secure these rights. In Editorial Board of Pravoye Delo and Shtekel v. Ukraine, the mentioned Court recognized that the risk of harm posed by communications on the internet to the exercise and enjoyment of human rights and freedoms, particularly the respect for private life, is certainly higher than that posed by the press. Therefore, "the policies, governing reproduction of materials from the printed media and the Internet may differ. The latter undeniably has to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned" (para. 63).

2. The rights of the child in the digital environment

Modern technologies influence the lives of adults, but their influence over children is far greater. These technologies have undoubtedly enhanced children's autonomy and independence. At the same time, children face many more risks of harm, which are now mediated and exacerbated online. Livingstone note that in its earliest days public policy regarding the protection of children on the Internet focused on inappropriate content and activity involving the sexual abuse of children. Both children's increased use of new technologies and their acquisition of sophisticated digital skills have helped increased awareness of the diversity of possible risks to them. This has shifted public perception away from viewing cyberspace as a distinct sphere in need of targeted regulation and toward growing acceptance that what is illegal or inappropriate offline should be the same online. This leaves policy makers and legislators with a difficult balancing act between supporting and empowering children online while at the same time protecting them at the same time [Livingstone S. and O'Neill B., 2014: 20].

[4] Factsheet — New Technologies. European Court of Human Rights, Press unit, March 2022.

In response to increased awareness of the risks that children face globally, the UN Committee on the Rights of the Child issued its General Comment No. 25 on children's rights in relation to the digital environment.[5] During the drafting process, the Committee received 132 submissions from 26 states, regional organizations, United Nations agencies, national human rights institutions, children's commissioners, child and adolescent groups, civil society organizations, academics, the private sector, and other entities and individuals expressing their views on the matter.[6] The document adopted explains how states should implement the UN Convention on the Rights of the Child (UNCRC) in relation to the digital environment. It refers to civil rights and freedoms, problems with violence against children, family environment and alternative care, children with disabilities, education, leisure and cultural activities and other specific issues, thus covering full range of rights provided for by the UNCRC.

The development of Council of Europe (CoE) legislation also takes into consideration the necessity to protect children from ICT-related risks. One major success was the Convention on Cybercrime (2001),[7] which became the first international treaty on crimes committed via the Internet and other computer networks. Due to its limited scope, child-related offenses covered under the treaty are limited exclusively to child pornography (Article 9). Other risks are considered in the CoE Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018). This document is based on assessing the best interests of the child and his or her evolving capacities, and it recommends that the governments of member states review their legislation, policies and practices to ensure that they promote the full array of the rights of the child. In particular, a comprehensive legal framework should provide for preventive and protective measures in relation to the digital environment. This is to provide support measures for parents and caretakers in order to prohibit all forms of violence, ex-

[5] CRC/C/GC/25 of 2 March 2021.

[6] The Council of Europe was among the bodies that made a submission. Based on the CoE Strategy for the Rights of the Child for the Period 2016–2021 (2016), which identified the rights of the child in the digital environment as one of its priority areas and recognised that children are entitled to receive support and guidance in their discovery and use of the ICT (paras. 56-61), it referred to the key rights which should be addressed by the pending General Comment. These include: the right to freedom of expression and information, the right to education, the right to participation, the right to engage in play, the right to assembly and association, the right to protection of privacy, data and identity, and the right to protection and safety.

[7] The Convention is open for accession by non-member states as well.

ploitation and abuse; to provide effective remedies as well as recovery and reintegration services; to establish child- and gender-sensitive counselling, reporting and complaint mechanisms; to encompass child-friendly mechanisms for consultation and participation; and to set up accountability mechanisms. The Guidelines thus reflect international recognition of a broad range of challenges to the rights of the child in the digital environment.

3. The privacy of the child: a new dimension for familiar concerns

Attention to the protection of children's privacy[8] on the Internet has recently been on the increase [Schreiber A., 2014: 13]; [Phippen A., 2017: 29]; [van der Hof S. and Lievens E., 2018: 33]. Although the right to privacy had been acknowledged from the outset, the UNCRC provides for it explicitly in Article 16, as its importance has been highlighted anew in the context of digital technologies. Morgan attributes this to a sharp increase in Internet usage by ever younger children together with the complexity of a technology-mediated environment [Morgan A., 2018: 44).[9] Privacy protection in such a complex environment has become a prerequisite for guaranteeing online child safety and therefore has begun to evolve as a separate, though interrelated, pillar within many online child safety initiatives [Macenaite M., 2016: 2].

Safety is indeed the most prevalent discourse in the field of child privacy protections. This risk is addressed on all levels through national guarantees [Balajanov E., 2018]; [Williams K., 2003] and international norms, including the CoE Convention on Cybercrime[10] and soft law such as the recent UNCRC Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child concerning the sale of children, child prostitution and child pornography.[11]

[8] Current conceptions of the right to privacy draw together three related aspects of privacy: informational privacy (right to control over information pertaining to a person, specifically preventing others from obtaining or using that information), constitutional, or decisional, privacy (the right to ability to make autonomous life choices without outside interference or intimidation (or without "being governed by the state" and physical privacy (the right to a private space and to bodily integrity (see UNICEF, 2017: 7 etc.).

[9] An estimated one third of Internet users across the globe are under 18 years old. These Internet users are operating in a world that was not originally designed with them in mind.

[10] The treaty is open for accession by non-member states as well. It became the first international treaty on crimes committed via the Internet and other computer networks.

[11] CRC/C/156 of 10 September 2019.

The ECtHR addressed online safety issues in K.U. v. Finland. The Court has noted that posting advertisements of a sexual nature about a twelve-year-old applicant was a criminal act that resulted in a child becoming a target for pedophiles and therefore called for a criminal law response that included an appropriate investigation and prosecution. The Court has noted too that new forms of communication required even greater prudence when the information is related to child privacy concerns. States have a positive obligation to establish a legislative framework to protect children in a timely manner from grave interference with their privacy (para. 49).

A new discourse addressing violations of data processing as part of protecting child privacy is quickly taking shape. The EU General Data Protection Regulation (GDPR)[12] offers a valuable addition to the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981),[13] which does not contain specific norms aimed at the protection of children but no doubt has a direct bearing on the issue. Atkinson notes that Recital 38 of the GDPR sets the overall tone for the treatment of a child's personal data when it says that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, safeguards, and of their rights in relation to the processing of personal data [Atkinson L., 2018: 31].

The ECtHR has not so far considered any data-processing cases where violations of a child's privacy is at issue. Apart from the safety-driven K.U. v. Finland, the Court has seen relatively few cases related to child privacy in general and even fewer that involve the digital environment. In Avilkina and Others v. Russia, confidential medical information about the applicants, one of whom was a minor, was disclosed by a medical facility following a request from the prosecutor's office. The Court reiterated that the protection of personal data, including medical information, is of fundamental importance to a person's enjoyment of their right to respect for their private and family life as guaranteed by Article 8 of the ECHR. The disclosure of such data may seriously affect a person's enjoyment of their private and family life, as well as their social and employment situations, by exposing them to opprobrium and the risk of ostracism (para. 45).

The effect of disclosing information on a child's reputation was considered in Aleksey Ovchinnikov v. Russia. The ECtHR reiterated that in

[12] The GDPR is not applicable to non-EU member states.

[13] A protocol amending the Convention for the Protection of Individuals with regard to the Processing of Personal Data was adopted by the Committee of Ministers at its 128th Session on 18 May 2018.

certain circumstances a restriction on reproducing information that has already entered the public domain may be justified. It concluded that the fact that the information about the child had already been disclosed by another newspaper and that the incident had been widely discussed in the press and on the internet was not relevant, because the child's reputation was at stake and "publication of the names of the juvenile offenders…did not make any contribution to a discussion of a matter of legitimate public concern" (paras. 50–52). This case is an important development of the Court's jurisprudence and confirms that a child's privacy must be protected not only in cases of a potential threat to safety, but also in order to respect their reputation. This is in line with Article 16 of the UNCRC, which states that, "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation."

The ECtHR will no doubt see more cases relating to child privacy issues in the future. Global and regional initiatives reflect social concerns and indicate an understanding that, as Baroness Kidron stated, "a child is a child until they reach maturity — not until they reach for their smartphone" [Kidron B., 2018: 26], and therefore children require special protection and care as much online as offline.

In the context of danger that children may bring on themselves when they use ICT [Altun D., 2019: 77][14] is linked to the role of parents as bearing primary responsibility for their children's media-related development and well-being. This is widely accepted in academic circles [Naab T., 2018: 94]; [Livingstone S. and Byrne J., 2018: 19] and by legislators. We can see this in para. 28 of the CoE Guidelines to respect, protect and fulfil the rights of the child in the digital environment that entrusts to parents the authority to decide if their child's data can be processed.[15] Lim speaks about the emergence of "new parenting obligations" necessary to ensure that parents "are the voices of authority to guide their children towards all that is edifying and beneficial in media, and to steer them away from that which is risky and harmful". This new kind of parenting, he notes, goes beyond traditional

[14] According to the studies only 58 out of 100 applications designed for preschool-aged children are appropriate for their level of development.

[15] The Guidelines emphasize that member states should ensure that their legal frameworks encompass the full range of unlawful acts that can be committed within the digital environment (para. 73-74 of the Guidelines). The reference to "the full range of unlawful acts" is particularly important bearing in mind the constant development of technologies. It provides an obligation to states to keep their legislations updated to address current threats to the rights of children.

childcare. It transcends the online sphere and extends to the offline interactions of the child. The question, however, is whether parents are ready and capable of embracing their new obligations [Lim S., 2018: 36].

Parents may not understand the nature of the risks encountered online [Livingstone S. and Byrne J., 2018: 25]. Much of the contemporary research on parenting in the digital environment, as well as conversations among parents themselves, focuses on keeping children safe from harm [Clark L. and Brites M., 2018: 81]. Parents are also concerned about the potential harm ICT may cause to children's emotional development, as well as about the addictive and time-consuming nature of these technologies [Altun D., 2019: 88]; but threats to their child's reputation is not something most parents routinely consider.

Another reason parents may be ineffective in this regard is because unlike modern "digital children" they were not born into these new technologies and have to learn for themselves how to manage them. They do not trust the integrity of security measures and privacy settings offered by social network sites, and they lack the skills needed to cope with them [Autenrieth V., 2018: 225]. Some authors for example [Livingstone S. and Byrne J., 2018: 23] note that parents who are less confident of their own or their child's digital skills take a more restrictive approach to mediating their children's online activities. In trying to keep their children safe, they not only deprive them of the opportunities that ICT offers but also impede the exercise of their rights to privacy and freedom of expression, and consequently they hamper their children's ability to seek outside help or advice when problems at home arise.

4. The privacy of the child: new risks

Excessive control by parents was until recently considered the main negative impact of their authority over their children's online activities [Livingstone S. and O'Neill B., 2014: 28]; [Atkinson L., 2018: 32]. However, they are now viewed as the main contributors to publicizing their children.[16] Parents leave a trace of their children in a digital space when they decide to share their child's personal information online or to share information about themselves that might directly or indirectly be linked to their child.[17]

[16] A digital footprint survey across ten European countries revealed that 81% of mothers digitally upload photographs of their children aged 0-2 years.

[17] Some 92% of children by the age of two years have an online presence due to their parents' disclosures.

The shared information may not only endanger the safety of the child; it may also undermine their dignity and reputation [Steinberg A., 2017: 848].[18] An illustrative example of this parental ignorance is the so-called "YouTube families", which make a show out of their daily routines and open up the lives of their children to the public in every possible detail.[19]

"Sharenting", the habitual use of social media to share news, images, etc. of one's children, frequently begins before birth with the uploading of fetal ultrasound photographs, and it has become tightly interwoven with parenting practices. Interestingly enough, the practice became widespread because it gave parents an opportunity for the (re) production of parental self-identity and social approval [Damkjaer M., 2018: 216], but now it is undergoing public criticism [Autenrieth V., 2018: 219].

Parents are not completely ignorant of the potential risks that posting information about their children online can bring. They fear "stranger danger" as well as the commercial misuse of their child's photos. They have exhibited some awareness that they need to consider the reactions of their children once they are old enough to know about the photos of them that their parents shared. The development of new photo practices that allow parents to display their children while maintaining some anonymity can be considered one strategy to mitigate these risks [Autenrieth V., 2018: 226]. Although parents understand their online actions can be a threat to their children's privacy and therefore try to manage it, most keep "sharenting" anyway [Bessant C., 2018: 7].

Damkjaer points out that in order to grasp the growing significance of sharenting we must acknowledge that parents' approaches to communication technologies do not spring from rational, intentional decision making. There is a broad range of reasons why parents sharent. It is true that some do this to earn income. However, most do it to receive information and guidance, build and maintain social relationships, and to develop a parental identity [Damkjaer M., 2018: 210, 211]. Becoming a parent entails major practical, emotional, social, and relational changes, not all of which can

[18] According to recent studies, 56% of parents shared (potentially) embarrassing information about their children online, 51% provided information that could lead to identification of their child's location at a given time, and 27% of participants shared (potentially) inappropriate photos.

[19] See, for example, the "8 Passengers" vlog by a family with six children. Available at: https://www.youtube.com/channel/UCQ3FRaHOIwXLOQNeUwVpBUA (accessed: 12.07.2019); the KBS show "The Return of Superman". Available at: https://www.youtube.com/playlist?list=PLMf7VY8La5RFIeOyIZ5IOm68WVb7c2dyT (accessed: 12.07. 2019)

be handled on one's own. The possibility of connecting with other parents and receiving positive personal support, whether emotional or practical, from the community is particularly important for families with medically fragile children. Whatever the reasons for sharenting are, it can instigate a conflict between parental rights and the right of children to their own privacy [Steinberg A., 2017: 842, 852]; [Bessant C., 2018: 7, 8].

Of all the current threats to the privacy of the child, the one created by parents' activities online seems to be the most difficult to address. Parents are presumed to play a key role in the protection of their children's rights, since they are ideally positioned to assess and address the particular "best interests" of their children [Livingstone S. and Byrne J., 2018: 27]. Measures developed to protect the privacy of the child are consequently framed within a paradigm of rendering support to parents, and not in the context of their obligation not to disclose information about their children.

5. Are we ready to regulate sharenting?

The sharenting phenomenon has been the object of numerous academic studies. It was found that parents' and guardians' online activities may cause damage to their children's privacy. While many parents are aware of the safety-related risks incurred by sharenting and try to mitigate them, threats to a child's reputation are mostly ignored. To address this problem, some national jurisdictions have made efforts to regulate sharenting.

In the US the infringement of children's privacy by parents can be considered as abuse. If the state can demonstrate that parental actions caused substantial harm to their child's well-being, it is authorized to intervene in such circumstances in order to protect children from the harm occurring in online forums. Authorities can seek a remedy through the courts or consider obtaining an injunction precluding the parents from posting additional harmful content online. Steinberg underscores that it is the state actor, not the child, who would bring forth this litigation. This remedy is not ideal as it is aimed only at parents who share the information. They can be required to delete offensive material from the internet sites they possess. However, it gives the authorities little control over the information shared on sites not possessed or controlled by the parent or where the material has been downloaded or shared by third parties [Steinberg A., 2017: 872].

A direct obligation of parents to protect the privacy of their children is stipulated by the privacy laws of contemporary France. Parents can be

prosecuted for publishing intimate details about their child. The penalty is very severe, tens of thousands of euros or up to a year in jail. While children may take their parents to court only upon attaining their majority, this regulation is nevertheless a significant step forward. When paired with suitable informational campaigns, it can cause parents to reconsider their behaviour.

The introduction of new parental obligations to protect the privacy of their children is currently being debated within United Kingdom academic circles [Oswald M., 2017: 3, 12]. However, UK law at present does not recognize a child's right to privacy in cases of infringement by their parents. Analyzing remedies that a child might use to prevent sharenting and to secure the removal of sharented information, Bessant points to a range of legal avenues potentially available to anyone who objects to the online dissemination of their personal, private or confidential information, including a breach of confidence action or a tort of misuse of private information. She notes that where a child's privacy has been violated by their parents, their ability in practice to obtain a remedy is in some regards potentially more limited than that of an adult. Children rarely have the financial means to bring court proceedings. Furthermore, they must prove that their information was confidential one, that the parent was subject to a duty of confidence, and that the sharenting was unjustified. Substantive as well as procedural legal hurdles help to explain why there is no substantial jurisprudence on this issue in the UK, and it "has yet to be seen how the English courts will respond to the new phenomenon of sharenting" [Bessant C., 2018: 20].

The United Kingdom Data Protection Act also has provisions for adjudication of children's privacy rights. Under this act a child may apply to the UK Information Commissioner's Office (ICO), requesting it to undertake an assessment to determine whether their personal data is being processed in breach of the Act. In cases where a parent has not sought the consent of the child to publish their private information online and the ICO concludes that there has been a serious breach of the data protection principles, it may serve an enforcement notice requiring the parents to delete the objectionable information. However, the law has placed the burden of initiating the process on the child. Children should ask their parents in writing to stop posting and/or to remove the information posted online within a specified period. The notice should state why the child believes continued online disclosure is causing or likely to cause them unwarranted and substantial damage or distress. If the parent ignores the notice, the child is entitled to seek assistance from the courts [Bessant C., 2018: 17–19]. Again, this

course of action would be too complicated procedurally for the average child to carry out [Clark L. and Brites M., 2018: 87].

While the United States and France have already introduced norms meant to combat harmful sharenting and the UK is anticipating the development of new practices within existing remedies, most countries are still debating certain aspects of the child's right to privacy [Ogrodnik-Kalita A., 2022:176][20] or are completely silent about the problem. Is it a problem that there is no child-friendly reporting and complaint mechanism, as recommended by CoE Guidelines to respect, protect and fulfil the rights of the child in the digital environment? Would the privacy of the child in fact be protected in case such a mechanism existed? We daresay it would not. The establishment of a child-friendly complaint mechanism is not a remedy in itself so long as the parents are considered only in their capacity as defenders of their children.

It would be an exaggeration to suggest that this perception is never questioned. The United Nations Committee on the Rights of the Child addressed these concerns while drafting its General Comment on children's rights in relation to the digital environment.[21] However, the reactions from the academic community, the NGO sector and international organizations have confirmed that parental authority is still considered critical, "in terms of recruiting the adults in children's lives as educators and as citizen participants in a global project that focuses on delivering children's rights across all aspects of young lives".

The text of the adopted document reflects this approach. While the General Comment has several paragraphs devoted to the issue of automatic processing of a child's data (paras. 70–72), the danger of parents sharing online is barely acknowledged. Parents are listed among other persons whose actions may be threatening to a child's privacy (para. 67) with no further elaboration on the legislative, administrative, and other measures states should take to ensure that children's privacy is respected and protected in this context. The General Comment stipulates the necessity of obtaining consent from the parent or caregiver in certain cases prior to processing child's data (para. 71). There is no mention of a possible conflict between a parent and a child on this issue or ways to resolve one. The stance taken

[20] In Poland, for example, the question of when a child is granted the right to privacy is contested.

[21] UNCRC. General Comment on Children's Rights in Relation to the Digital Environment Concept Note. Mode of access. Available at: https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx, (accessed: 03.07.2019]

by the UN Committee on the Rights of the Child with regard to sharenting should serve as a demonstration of the power of the traditional cultural perceptions that reinforce understanding the child as incontestably an object of care and rule by their parents [Livingstone S. and O'Neill B., 2014: 30].

Conclusion

The rapid development of digital technologies has unquestionably changed humanity daily life. They have brought about new possibilities for exercising and protecting human rights, but at the same time the possibilities for human rights violations have also grown exponentially. In order to address the new risks, the law and policies aimed at protecting human rights need to be adjusted in response to ICT's specific features.

Of all the contemporary threats to the privacy of children, the one created by parental activity online seems to be the most difficult to address. Parents are presumed to play a key role in the protection of their children's rights. Measures developed to protect children's privacy reflect the strong tradition of respecting parental rights to control and shape the lives of their children. Though some national jurisdictions have made some effort to provide legal remedies for children in case of a conflict between their rights and the rights of their parents, the international community seems to be unprepared to move away from the basic premise that the only role of parents is to guide and support children in the exercise of their rights. This is demonstrated by the position taken by the UN Committee on the Rights of the Child with regard to sharenting in its recent General Comment on children's rights in relation to the digital environment.

In the absence of a strongly articulated position from the main international body charged with setting child protection standards that apply to defending the right of the child to privacy against their parents, it would be unreasonable to expect a unified response to this new risk to child's privacy at the national level. It can be confidently stated that we are not yet ready (at both the national and international level) to regulate sharenting.

References

1. Altun D. (2019) An investigation of preschool children's digital footprints and screen times, and of parents' sharenting and digital parenting roles. *The International Journal of Eurasia Social Sciences*, vol. 10 (35), pp. 76–97.

2. Atkinson L. (2018) Interpreting the child-related provisions of the GDPR. *The Communications Law*, vol. 23, no.1, pp. 31–32.

3. Autenrieth U. (2018) Family photography in a networked age. Anti-sharenting as a reaction to risk assessment and behaviour adaption. In: G. Mascheroni, C. Ponte and A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age. Göteborg: Nordicom Press, pp. 219–231.

4. Balajanov E. (2018) Setting the minimum age of criminal responsibility for cybercrime. *The International Review of Law, Computers and Technology*, vol. 32, no.1, pp. 2–20.

5. Bessant C. (2018) Sharenting: balancing the conflicting rights of parents and children. *The Communications Law,* vol. 23, no 1, pp. 7–24.

6. Coccoli J. (2017) The challenges of new technologies in the implementation of human rights: an analysis of some critical issues in the digital era. *Peace Human Rights Governance*, vol. 1, no. 2, pp. 223–250.

7. Damkjaer M. (2018) Sharenting = good parenting? Four parental approaches to sharenting on Facebook. In: G. Mascheroni, C. Ponte and A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age. Göteborg: Nordicom Press, pp. 209–218.

8. Kidron B. (2018) Are children more than "clickbait" in the 21st century? *The Communications Law*, vol. 23, no.1, pp. 25–30.

9. Lim S. (2018) Transcendent parenting in digitally connected families. When the technological meets the social. In: G. Mascheroni, C. Ponte and A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age. Göteborg: Nordicom, pp. 31–39.

10. Livingstone S. and Byrne J. (2018) Parenting in the digital age. The challenges of parental responsibility in comparative perspective. In: G. Mascheroni, C. Ponte and A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age. Göteborg: Nordicom Press, pp. 19–30.

11. Livingstone S. and O'Neill B. (2014) Children's rights online: challenges, dilemmas and emerging directions. In: S. van der Hof, B. van den Berg and B. Schermer (eds.) Minding Minors Wandering the Web: Regulating Online Child Safety. Berlin: Springer, pp. 19–38.

12. Macenaite M. (2016) Protecting children's privacy online: A critical look to four European self-regulatory initiatives. *The European Journal of Law and Technology*, vol. 7, no. 2, pp. 1–26.

13. Morgan A. (2018) The transparency challenge: Making children aware of their data protection rights and the risks online. *The Communications Law*, vol. 23, no.1, pp. 44–47.

14. Naab T. (2018) From media trusteeship to parental mediation: The parental development of parental mediation. In: G. Mascheroni, C. Ponte and A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age. Göteborg: Nordicom Press, pp. 93–102.

15. Ogrodnik-Kalita A. (2022) Protection of the child's right to privacy in the Convention on the Rights of the Child, the General Data Protection Regulation and Polish law. In: E. Marrus and P. Laufer-Ukeles (eds.) Global Reflections on Children's Rights and the Law: 30 Years after the Convention on the Rights of the Child. New York: Routledge, pp. 171–181.

16. Oswald M. et al. (2017) Have «Generation Tagged» lost their privacy? University of Winchester: Centre for Information Rights. Available at: https://cris.winchester.ac.uk/ws/portalfiles/portal/356432/826826_Oswald_GenerationTagged_original.pdf (accessed: 4.01.2022)

17. Phippen A. (2017) Online technology and very young children: Stakeholder responsibilities and children's rights, *The International Journal of Birth and Parent Education*, vol. 5, no.1, pp. 29–32.

18. Clark L. and Brites M. (2018) Differing parental approaches to cultivating youth citizenship. In: G. Mascheroni, C. Ponte and A. Jorge (eds.) Digital Parenting: The Challenges for Families in the Digital Age. Göteborg: Nordicom Press, pp. 81–89.

19. Schreiber A. (2014) Family-based rights in privacy and other areas of law — an Israeli perspective. *The International Family Law, Policy and Practice*, vol. 2, no. 2, pp. 13–27.

20. Steinberg S. (2017) Sharenting: Children's privacy in the age of social media. *Emory Law Journal*, vol. 66, pp. 839–884.

21. Trajkovska M. L. (2015) Privacy, freedom of expression and the Internet. In: Essays in Honour of Dean Spielmann. Oisterwijk: Wolf Legal Publishers, pp. 335–342.

22. The Privacy, Protection of Personal Information and Reputation (2017) UNICEF Discussion Paper: Children's Rights and Business in a Digital World. Available at: https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf (accessed: 08.04.2022)

23. Van der Hof S. and Lievens E. (2018) The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. *The Communications Law*, vol. 23, no.1, pp. 33–43.

24. Wildhaber L. (2004) The European Court of Human Rights in action. *The Ritsumeikan Law Review*, vol. 21, pp. 83–92.

25. Williams K. (2003) On Controlling Internet Child Pornography and Protecting the Child. *Information and Communications Technology Law*, vol. 12, no.1, pp. 3 –24.

Information about the author:

N.V. Kravchuk — Senior Researcher, Candidate of Sciences (Law).

The article was submitted to the editorial office 18.04.2022; approved after reviewing 17.05.2022; accepted for publication 19.05.2022.

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

Research article
УДК 343.98.065
DOI:10.17323/2713-2749.2022.2.90.115

Automation of Forensic Authorship Attribution: Problems and Prospects

Tatiana Vladimirovna Romanova[1], Anna Yurievna Khomenko[2]

[1] Department of Humanities, National Research University Higher School of Economics, 25/12 Bolshaya Pechyorskaya Str., Nizhny Novgorod 603155, Russia, tvromanova@hse.ru, ORCID: 0000-0002-1833-2711

[2] Department of Humanities, National Research University Higher School of Economics, 25/12 Bolshaya Pechyorskaya Str., Nizhny Novgorod 603155, Russia, akhomenko@hse.ru, ORCID: 0000-0003-3564-6293

Abstract

The article deals with validation of an integrative attribution algorithm based on the analysis of the author's idiostyle using methods of interpretative linguistics with objectification of the available data with the help of mathematical statistics. The algorithm addresses the identification problem of the attribution. The choice of parameters describing the individual style of an author assumes that the text is a product of an authentic language personality described by psycholinguistic (Yu.N. Karaulov), sociolinguistic and forensic linguistic (S.M. Vul, M. Coulthard, R. Shuy) methods. To validate a hypothesis that the identification problem of attribution is best resolved by the integrative methodology, we have created the KhoRom application which brings together the aforementioned approaches to the analysis of language personality: http://khorom-attribution.ru/#/. It can be used to compare two language personality models and determine to what extent they are similar using the following metrics: Pearson correlation coefficient, linear regression determination coefficient and Student's t-criterion. Importantly, this application also describes the interpreted model of language personality to inform the user on the importance of values of each parameter. The system has a wealth of features, with the user able to choose parameters, view parameter implementation in the document and edit the final list of parameter implementations (in case of malfunction, the application performance can be corrected manually). The created application is only a part of the attribution algorithm. The data produced by mathematical statistics need to be analyzed by expert judgment through the use of

methodological recommendations developed for the algorithm. The effectiveness of this methodology has been proved by its validation on texts of various length and genres, with a number of documents pertaining to fiction, journalism, official and colloquial styles being analyzed. For texts of all discourses except colloquial, the developed algorithm has demonstrated a high level of accuracy (F-score of 0.8 to 1). For better applicability of the algorithm to colloquial texts, the authors have developed a number of improvements pending implementation.

Keywords

attribution, language personality, automated text processing, linguistic model, mathematical model, attributive software, forensic authorship attribution.

Acknowledgments: The study was performed with financial support of the Russian Fundamental Fund of Researches as part of research project No. 19-312-90022.

For citation: Romanova T.V., Khomenko A.Yu. (2022) Automation of Forensic Authorship Attribution: Problems and Prospects. *Legal Issues in the Digital Age*, vol. 3, no. 2, pp. 90–115. DOI: 10.17323/2713-2749.2022.2.90.115

1. Background

At present stage of progress in science a problem of automation of social processes has been discussed by specialists in all fields including forensic experts. "Forensic investigation means a procedural activity involving studies and opinions to be given by experts on issues which require specific knowledge in the area of science, technology, arts or crafts and which courts, judges, investigative authorities, inquiry officers, investigators or public prosecutors deal with in order to ascertain the circumstances to be proved as part of a specific case"[1]. A forensic investigation can be both criminal and non-criminal. While automated analytical tools have become customary for most criminal investigations (trace examinations, forensic genetics etc), software support is not yet available to all investigations of this kind in Russia. Thus, forensic authorship attribution is an inquiry associated with criminal investigations (classified as such by the Russian Ministry of Justice)[2], its purpose

[1] Federal Law No. 73-FZ "On State Forensic Investigations in the Russian Federation" dated 31 May 2001. Rossiyskaya Gazeta, No. 256 of 31.12.2001. Available at: URL: https://base.garant.ru/12123142/ (accessed: 03.05.2020)

[2] Order No. 237 "On Approving the List of Forensic Inquiry Types to Be Performed at Federal Offices of Forensic Services under the Ministry of Justice, and the List of Practitioners Authorized to Perform Investigations at Federal Offices of Forensic Services under the Ministry of Justice" of 27 December 2012 (as amended of 13 September 2018). Available at: URL: www.pravo.gov.ru (accessed: 03.05.2020)

being to attribute a text to a specific author (group of authors) or obtain information on individual authors. However, the extent of automation of this kind of inquiry is currently quite low. This is probably due to the fact that courts will often dismiss the requests for investigation of this kind.[3]

2. Problems and prospects of developing algorithms for automated forensic authorship attribution

2.1. Principles of authorship attribution in and outside Russia

In modern linguistics, automated analytical methods for textual attribution for purely research purposes are progressing worldwide. They are implemented as software products both in and outside Russia, the most popular still being models and algorithms based on n-gram speech recognition [Bacciu A., Morgia M., 2019]; [Litvinova T., Sboev A., Panicheva E.B., 2018: 167–169]; [Custódio J., Paraboni I., 2018]; [Murauer B., Tschuggnall M., Specht G., 2018]; [Muttenthaler L., Lucas G., Amann J., 2019], part-of-speech attribution of units [Litvinova T., Sboev A., Panicheva E.B., 2018: 177], variable length patterns [Custódio J., Paraboni I., 2018] and using cluster analysis [Panicheva P. et al., 2018], traditional [Gomzin A. et al., 2018] and modified [Korobov M., 2015: 320–332] Python libraries, vector transformation algorithms [Bacciu A., Morgia M., 2019] etc. There have been successful attempts to use linguistic models as such to determine who authored a text (based on the vector approach to analysis). As regards Russian software products, the following are worth mentioning.

M.A. Marusenko software based on the theory of image recognition. This approach to attribution of language personality could be seen in his studies [Marusenko M.A., 1990, 2003] and E.S. Rodionova [Rodionova 2008 a,b] focused on the analysis of deep text structures are best reflects the peculiarities of a person's cognitive processes. Such an approach will doubtlessly produce decent results due to the model being more complete and deductive and better reflecting the subject of study. Nevertheless, the model is extremely difficult to use and understand for anyone who doesn't have the theoretical knowledge of image recognition and mathematical statistics. The use of this model is still further complicated by the absence of

[3] The Court on Intellectual Property Rights of the Russian Federation, ruling of 4 December 2020 on case No. SIP-676/2019; The Court on Intellectual Property Rights, ruling of 29 November 2019, case No. SIP-695/2019. Appellate ruling of 26 December 2018. No 203–APU 18–25 etc. Available at: URL: https://base.garant.ru/75013773 (accessed: 03.05.2020)

a generally accessible user interface while repetition of all mathematical transformations described therein is very lengthy.

V.N. Zakharov software (Atributsia) based on the analysis of grammar and syntax [Zakharov V.N. et al., 2000] that allows to parse literary text using multiple linguistic features. The software consists of two parts: the grammatical analysis module and the syntactic analysis module. They enable to partially automate and formalize the parsing process across 69 parameters [Sidorov Ju. B. et al., 1999: 66]. However, this software requires the involvement of an expert philologist to check the correctness of part-of-speech attribution etc. V.N. Zakharov and his colleagues analyzed the works of Fyodor Dostoevsky and non-attributed texts of still disputed authorship. As a result of the experiments, this group of researchers has managed to identify certain anonymous texts as those authored by Dostoevsky and thus make them part of the classical author's literary heritage.

A.N. Timashev software (Attributor) based on letter triads [Timashev A.N., 2007]. That researcher has proposed to use three-letter combinations — triads — as a criteria to distinguish an author's style. This approach includes single-letter and twin-letter function words into the analysis as making up a "significant part of the frequently used prepositions, conjunctions, particles and interjections traditionally believed to be meaningful style defining features" [Batura T.V., 2012: 87]. The above methodology uses a text database of 103 Russian authors of 19–20th centuries. At the start, the software uses a machine learning method involving an expert linguist. To avoid the errors resulting from a comparison of statistically non-comparable objects, the text should be at least 6 pages long.

A.S. Romanov software (Avtoroved) based on the support vector machine in the form of the most frequently used trigrams and words [Romanov A.S., 2010]. The authorship problem is regarded as a classification problem to be solved using the support vector machine where the idiostyle is described with symbol trigrams and words most frequently used in Russian. The main findings were produced on a set of 215 prose texts by 50 Russian writers borrowed from M. Moshkov's e-library. For texts authored by 2/5/10 persons, the experiments showed the most informative authorship features to be those restricted to 300–700 most frequent trigrams and 500 most frequently used words. The methodology proved to be practically useful for analysis of short electronic messages (which is remarkable since dealing with short texts is extremely complicated) when the software nicknamed Avtoroved and the underlying methodology were tested at a military base. The findings showed that in case of two potential authors the authorship of

100-symbol long texts could be attributed with a maximum accuracy of 0.76 ± 0.11. A sub-problem to identify the author of a web forum message was solved with an accuracy of 0.89 ± 0.08. Thus, the said method works relatively well for short e-messages which offers high experimental potential in the context of modern electronic communications.

KAT software was produced by N.I. Lobachevsky State University, Nizhny Novgorod. This product uses a database of Russian classical texts (written by Leo Tolstoy, Nikolai Gogol, Ivan Turgenev), with models relying on an analysis of coefficients of correlation between different parts of speech (after B.N. Golovin) [Radbil T.V., Markina M.V., 2019]. The use of such coefficients is undoubtedly well-founded from a psycholinguistic and behavioral perspective offered by fundamental science since the part-of-speech association of vocabulary of an author's idiolect is clearly a distinctive feature of style. Importantly, the software uses not just a transversal coefficient of correlation between all parts of speech but conscious relationships between them.

Lingster 3.0 software by the Institute of Forensic Science under the Federal Security Service [Rubtsova I.I., Ermolayeva E.I., Bezrukova M. Yu. et al., 2007], TextAnalyst 2.0 by the Moscow Research Center [Ionova S.V., Ogorelkov I.V., 2020]; RusIdiolect database by the laboratory of corpus ideolectology, Voronezh State Pedagogical University [Litvinova T.A., Gromova A.V., 2020: 77– 88].

Due to specifics of the legal practice, the principles of forensic authorship attribution somewhat differ from those applicable to solution of research problems as such. This follows in the first place from the Russian law: Federal Law No. 73-FZ "On State Forensic Investigations in the Russian Federation" of 31 May 2001 ("Law No.73-FZ)[4] and all codes establishing procedural standards (for criminal, arbitration and civil procedures and administrative offenses)[5] provide for personal liability of experts in respect of an opinion to be given. "An expert's opinion is a written document reflecting

[4] Available at: URL: http://www.consultant.ru/document/cons_doc_LAW_31871/ (accessed: 12.06.2020)

[5] 1) Code of Criminal Procedure of Russian Federation dated 18.12.2001, Federal Law No 174-FZ(as amended on 25.03.2022 and including modifications in force from 19.05.2022). Available at: URL: http://www.consultant.ru/document/Cons_doc_law_34481/ (accessed: 24.05.2022)

2) Code of Arbitration Procedure of Russian Federation dated 24.07.2002, Federal Law No 95-FZ (as amended on 30.12.2021, as modified on 10.01.2022}. Available at: URL: http://www.consultant.ru/document/cons_doc_LAW_37800/ (accessed: 24.05.2022)

3) Code of Civil Procedure of Russian Federation dated 14.11.2002, Federal Law No 138-FZ (as amended on 16.04.2022). Available at: URL: http://www.consultant.ru/document/Cons_doc_LAW_39570/ (accessed: 24.05.2022)

the course and findings of investigations conducted by the expert [italics added. — T.R., A.Kh.]"[6]. While this liability cannot be shifted to the machine, the expert should critically analyze the findings produced by the software (if any) and issue a "well-founded and objective opinion"[7] "within the ambit of the respective qualifications, comprehensively and to the full extent"[8]. Any failure to comply with requirements of the law will incur not only moral liability before the civil society for the opinion being issued but also criminal liability before the state under Article 307 of the Criminal Code of Russia[9].

Since the expert's personal liability is established by law, this constitutes an obstacle preventing the use of fully automated technologies of attribution analysis in Russian legal practice. But this obstacle is not the only one. A specific feature of the national regulatory framework including the codes of criminal procedure, civil procedure, arbitration procedure and administrative offenses, and Federal Law No. 73-FZ (Article 8), is that the expert dealing with questions to be explored should strictly remain within the ambit of his competence as determined by the amount of his expertise: "The expert may <…> 4) provide an opinion within his competence [italics added. — T.R., A.Kh.,] including on issues relevant to the subject of expert investigation though not mentioned in the order on forensic investigation"[10]. The same idea is present in the codes of civil procedure[11], arbitration procedure[12] and administrative offenses[13].

---

4) Code of Administrative Offenses of Russian Federation dated 30.12.2001, Federal Law No 195-FZ (as amended on 16.04.2022 and modified on 17.05.2022, including amendments and modifications in force from 27.04.2022). Available at: URL: http://www.consultant.ru/document/cons_doc_law_34661/ (accessed: 24.05.2022)

[6] Federal Law No. 73-FZ "On State Forensic Investigations in Russia" dated 31 May 2001. Rossiyskaya Gazeta. No 256 of 31.12.2001. P.9. Available at: URL: https://base.garant.ru/12123142/ (accessed: 03.05.2020)

[7] Ibid. P.8. Available at: URL: https://base.garant.ru/12123142/ (accessed: 03.05.2020)

[8] Ibid. P.9. Available at: URL: https://base.garant.ru/12123142/ (accessed: 03.05.2020)

[9] Criminal Code of Russian Federation dated 13.06.1996, Federal Law No. 63-FZ. Available at: URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (accessed: 03.05.2020)

[10] Code of Criminal Procedure of Russian Federation dated 18.12.2001, No 174-FZ. Available at: URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (accessed: 03.05.2020)

[11] Code of Civil Procedure of Russian Federation dated 14.11.2002, No 138-FZ. Available at: URL: http://www.consultant.ru/document/cons_doc_LAW_39570/ (accessed: 03.05.2020)

[12] Code of Arbitration Procedure of Russian Federation dated 24.07.2002, No 95-FZ. Available at: URL: http://www.consultant.ru/document/cons_doc_LAW_37800/ (accessed: 03.05.2020)

[13] Code of Administrative Offenses of Russian Federation dated 30.12.2001, No 195-FZ. Available at: URL: http://www.consultant.ru/document/cons_doc_LAW_34661/ (accessed: 03.05.2020)

"An expert's professional competence (from Latin competo — achieve, fit, correspond) assumes a set of theoretical, methodological and practical knowledge of expert investigation of a particular kind and type"[14] . The experts performing forensic authorship attribution will normally have basic linguistic or philological education and subject-specific retraining on investigation of speech language activity products and/or (preferably) investigation of written speech for attribution of authorship (in accordance with the Ministry of Justice classification)[15]. This background does not assume expertise in the field of big data, probability theory, machine learning and neural networks, mathematical statistics, image recognition theory, vector theory etc., as disciplines required to master and understand the software relying on the best performing algorithms for automatic identification of authors of written documents. Hence, the Russian Federation law on forensic investigation fundamentally (via provisions enshrined in the codes of procedure, federal laws, departmental instructions and orders) restricts the use of purely computer technologies in authorship attribution investigations, so that experts cannot rely on software alone to draw a conclusion as, for example, in the case of genetic investigation. Naturally, experts cannot use the software based on the principles they don't understand for lack of special knowledge of statistics, mathematics, probability theory etc.

Apart from the law, the use of automated technologies to identify the author of a text is restricted by virtue of the national scientific tradition related to a wide dissemination of the interpretative research paradigm in philology in general and in forensic linguistics in particular. Thus, forensic attribution methodologies proceed from the ideas proposed by S.M. Vul [Vul S.M., 2007] and further elaborated by A.Yu. Komissarov [Komissarov A.Yu., 2000]; E.I. Goroshko [Goroshko E.I., 2003: 221–226]; E.I. Galiashina and E. I. Ermolova [Galashina E.I., Ermolova E. I., 2005: 20–22]. They are based on the theory of distinctive style shaped by a certain social environment and cognitive processes unique for each person. The work under the title Comprehensive Methodology of Authorship Attribution [Rubtsova I.I., Ermolayeva E.I., Bezrukova A.I. et al., 2007] is currently one of the relevant institutional methodologies.

[14] Encyclopedia of Forensic Investigations. Moscow, 1999. P. 177.

[15] Order No. 237 "On Approving the List of Types of Forensic Investigations to be Performed at Federal Offices of Forensic Services under the Ministry of Justice, and the List of Practitioners Authorized to Perform Investigations at Federal Offices of Forensic Services under the Ministry of Justice" dated 27 December 2012 (as amended of 13 September 2018). Available at: URL: www.pravo.gov.ru (accessed: 03.05.2020)

The practice of automatic text attribution in Russia is currently borrowed from the West European and North American schools of thought where authorship identification has been traditionally — from L. Campbell [Campbell L., 1867] down to modern day [Koppel M., Schler G., 2003: 72–80]; [Wright D., 2007: 212–241] etc. — related to methodologies of computational stylometry. Meanwhile, these schools have a tradition similar to that existing in Russia, that is, the use of properly linguistic, qualitative text attribution techniques/methodologies [McMenamin G., 2002], with forensic authorship identification practices relying on the idiolect theory [Coulthard M., 2004: 447]. In the Western tradition, idiolect has always been perceived as a construct which represents "not merely what a speaker says at one time: it is everything that he could say in a given language" [Bloch B., 1948: 3–46]. For an English speaker, a major parameter defining the idiolect is the speaker's social status. The language style is linked to linguistic variability that follows from social context. A language style offers two types of choice: variation within or deviation from the established norm. A change within the limits of a norm assumes a choice of grammatically acceptable ("correct") forms (twenty-six/twenty six/26) while a deviation from the norm assumes a choice that covers grammatically wrong or inacceptable ("incorrect") forms (I might go/I could go/I might could go/I might could did go). A norm can be described in terms of both linguistics and statistics. Linguistic norms assumed in the use and perception of a language are described in detail in dictionaries and grammar books. Statistical norms are those that reflect the linguistic norm in the form of a certain frequency distribution of each form within the population of particular native speakers [McMenamin G., 2002].

Courts in certain parts of the USA and the UK (once a permission in respect of a particular case is given) will accept attribution investigations of quantitative content [Juola P., 2006: 233-334] involving the use of a software. A number of examples could be cited: Court of Appeal, London, 1991: the Queen vs. Thomas McCrossen; Leicester Crown Court, 1992: the Queen vs. Frank Beck. However, the use of fully automated investigations for forensic attribution in the West is an exception rather than rule. In Russia, as was noted above, this practice is altogether absent. Overall, courts in Russia will not often order an investigation to attribute authorship of a text. Authorship attribution investigations are frequent in respect of music and art[16] and

[16] The Court on Intellectual Property Rights, ruling of 4 March 2019 on case No. A63-22578/2017; The Court on Intellectual Property Rights, ruling of 18 June 2019 on case No. A40-224162/2017; The Court on Intellectual Property Rights, ruling of 13 January 2020 on case No. A57-15203/2018, etc.

much less so in respect of texts[17]. In criminal investigations, text attribution is ordered more frequently[18]; however, given the complex matters to be explored and the probability of making wrong conclusions in the absence of knowledge necessary for their assessment, we believe this happens less often than required.

In the English-language forensic linguistics, the principal event of automatic text processing to identify authorship and other individual features of a language personality is apparently a series of PAN events of the Conference and Labs of the Evaluation Forum or Cross-Language Evaluation Forum[19] in which researchers from Russia — such as Tatiana Litvinova of Rus Profiling Lab [Litvinova T.A. et al., 2017: 1–7] — are also involved. It is worth noting, however, that Rus Profiling Lab is virtually the only organization in Russia engaged on a permanent, professional basis in developing open-source, publicly available automatic attribution algorithms for Russian-language texts including for forensic purposes. A.S. Romanov and his team from the Tomsk State University of Control Systems and Radioelectronics [Romanov A.S. et al., 2021: 1–16] are currently working on improvements for the already available Avtoroved software in the interest of high-security institutions.

Despite the strongly prominent tradition of interpretative linguistics at both Russian-language and English-language forensic attribution schools, the preference for qualitative methods owes itself not so much to persistence of traditions in this branch of linguistics as to the law which makes experts personally liable for their opinions (in and outside Russia) before the civil society and the state. Importantly, no validated and commonly recommended methodology of automatic (computer-assisted) attribution analysis based only on statistics retrieved from the text is now available on a full scale either in Russia or elsewhere. The reason is the complexity of texts to be analyzed which may largely differ in terms of length, functional style, metadata affecting their structure etc. At this stage, given a lack of

[17] Determination of 20 July 2020 on case No. SIP-250/2017 to suspend proceedings and conduct an investigation.

[18] Order of 05 September 2018 by R.R. Saifetdinov, investigator of criminal investigation unit No. 6, Sverdlovsk Oblast office, Ministry of Interior, under criminal case No. 11801650081000303; order of 15 June 2018 by E.A. Nikiforova, senior investigator of the investigation unit, Noyabrsk office, Ministry of Interior, under criminal case No. 11701711492002633; order of 22 February 2017 by F.V. Tyutnev, senior investigator of the investigation unit, Volga Federal District office, Ministry of Interior, under criminal case No. 11701000150103930 etc.

[19] Available at: https://pan.webis.de. (accessed: 10.05.2022)

a shared, generally accepted and commonly recommended automatic research algorithm for attribution of texts and the current legal provisions in Russia, experts cannot apply strictly statistical methods, unless they are supported by interpretative approaches.

2.2. The prospects of forensic authorship attribution in Russia

Due to peculiarities of the Russian regulatory framework which provides for experts' personal liability before the state for the judgment they make, inadequate software implementation of automatic attribution algorithms with the resulting low accuracy for forensic purposes, and the strong tradition of interpretative linguistics, on the one hand, and imminent digitization of all spheres of social life, on the other hand, the only way forward for forensic attribution in Russia is, in our view, the integration of computer-assisted methodologies of quantitative text analysis with interpretative qualitative investigations performed by experts in a single software package. Obviously, there have been efforts to do that [Baranov A.N., 2001]; [Ionova S.V., Ogorelkov I.V., 2020: 115–127], and it is logical to move on.

The main purpose of this study is to develop an integrative text attribution methodology including formalization of language personality attribution models in order to make the algorithm adaptable to: a) computer-assisted implementation; b) wide range of linguists including forensic experts. The study is expected to result in an operational algorithm prototype for automatic/semi-automatic identification of authors of written texts.

2.3. Integrative attribution software

At the moment, the authors have tested a prototype methodology with the said parameters where the interpretative linguistic methods identify the information on the author's competences in the traditional sense (thesaurus and pragmaticon of a language personality, levels of mastering written speech competencies) while the stylystatistics allows to add objectivity to the findings of interpretative analysis. The KhoRom attribution resource prototype is available in the Internet[20].

The prototype solves the identification problem of attribution linguistics of the "sample comparison" type where one or more texts of unknown authorship and a sample text of known authorship are available. The method-

[20] Available at: URL: http://khorom-attribution.ru/#/ (accessed: 24.04.2022)

ology was tested on authorized texts to check its functional capability and ensure successful application as a forensic tool.

The proposed methodology implements the following algorithm. It will: automatically retrieve parameters describing the author's pragmaticon, thesaurus and lexicon; search for traditional stylometric data (text statistics data); assign a weight to each parameter; construct mathematical models of the compared texts; compare the mathematical models; perform expert analysis of statistical data. Importantly, this is not the authentic way to automatically attribute authorship but an integrative methodological concept bridging two approaches to objectify the interpretation with statistics followed by analysis of statistical data.

The formalization of multi-level structure of a language personality is based on the postulates of Yu. N. Karaulov's theory [Karaulov Yu. N., 2010] where a language personality is understood as a set of communicative skills (ability to produce oral speech and written texts, level of verbal communication culture, ability to achieve the purpose of communication etc.) acquired by the individual in a certain social environment during the period of development. In fact, the formalization process follows the principles of semantic syntax [Paducheva E.B., 1974] and Russian grammar rules[21].

The structure of language personality is regarded as a combination of three levels: verbal semantic, linguo-cognitive and motivational [Karaulov Yu.N., 2010].

A language personality is understood as a result of development in a certain social environment based on autobiographic, sociolinguistic and juridical linguistic approaches [Vinogradov V.V., 1961]; [Coulthard M., 2004: 431]; [Shuy R., 2005]; [Vul S.M., 2007].

Based on empirical study of 10 text fragments totaling 116 thousand words we have identified a number of language personality parameters that are invariably important as components of individual style, original authentic language, explicit feature of the author's language personality and at the same time are automatically retrievable from the text with minimum pre-processing required. For computer-assisted retrieval, all formal rules were programmed and incorporated into the KhoRom linguistic resource: http://khorom-attribution.ru/#/.

As a result of empirical study, the search parameters such as attribution of words to different parts of speech (number of content words, ratio

[21] The Russian Grammar. Available at: URL: htpp://rusgram.narod.ru/index.html (accessed: 16.11.2020)

of different parts of speech — legibility index, objectness coefficient etc.), average word lengths, presence/absence of compound hyphenated words, modal particles, interjections, presence/absence of "-to" modal postfix, preferable intensifiers were programmed at the verbal semantic level. The formalized search of units at this level is carried out in accordance with the text's morphological profile, that is, by tagging each word as a part of speech and all grammatical categories associated with the given part of speech. For instance, a search of elements with "-to" modal postfix will follow this algorithm:

1) + Prnt-to

2) — SPRO, nom / gen / dat / acc/ ins / loc / voc / gen2 / acc2 / loc2, sin / pl

3) — APRO, nom / gen / dat / acc/ ins / loc / voc / gen2 / acc2 / loc2, sin / pl[22].

Thus, the diagram can be read as follows: the search is for any part of speech with "-to" modal postfix (except pronouns and adjective pronouns) in any case of singular or plural.

Intensifiers are understood as words used to identify the extent of semantic category of intensity. These are mostly adverbs whose range is limited albeit great (in the modern discourse — ochen, silno, adski [very, strongly, damned]). But the category of intensity is not limited to exclusively adverbial content, for example: Kakaya krasota! [What a beauty!]. In this case, it is the pronoun kakaya that serves as an intensifier. Thus, a code of rules was developed as part of the study to search for structures with intensifiers; the list of intensifiers includes both adverbs with certain grammatical limitations (structures where the adverb does not express the category of intensity: for instance, it makes part of a compound nominal predicate, such as in On chuvstvuyet sebya khorosho [He feels good] and certain adjectives and pronouns in relevant grammatical structures such as: A "nastoyaschy", nom / acc, sin / pl + N: nastoyaschy bardak [real mess].

Regarding the search for parameters of the verbal semantic level, a total of 107 authentic rules were developed to identify 11 different structures in the text. The search for chosen parameters at this level, that of idiolect in accordance with the concept, is easy to formalize since the verbal semantic level has "more formal language features a priori believed to be stable

[22] Hereinafter the designations corresponding to part-of-speech tagging of the Russian National Corpus are used. Available at: URL: https://ruscorpora.ru/new/corpora-morph.html (accessed: 24.05.2022); «/» — or, «+» — presence of several elements in the structure; A — adjective, N — noun;

though the issue of their stability has not been specifically explored" [Litvinova T.A., 2019: 2].

To represent a fragment of personal thesaurus, we have chosen parameters such as key lexemes, frequently used word trigrams and bigrams, and explicators of axiological text dominants of the friend-foe dichotomy.

The key lexemes are identified using the logarithmic plausibility algorithm as the text of interest is compared to a large reference database (Opencorpora was used, URL: http://opencorpora.org, accessed 08.02.2020, 1,540,034 words as of the access date). As a result, a list of key words with numerical explication of the measure of logarithmic plausibility (loglikelihood score or LL) is generated for each text. The final list has only the words with LL value higher than 50.

A search for word bigrams and trigrams is based on the absolute frequency of finding words next to each other and is implemented using the functions of the chosen programming language. The most frequent word combinations for the texts in question are identified after the above preprocessing. The calculation also takes into account whether a given word is not in the list of stop words, words spelled in Cyrillic and those longer than 2 symbols. As a result of comparing two texts, a list of the most frequent word combinations is generated for each.

In analyzing key lexemes and most frequent word combinations, those with proper names are deleted from the resulting lists since these lexemes identify the thematic association of text rather than features of the author's idiostyle.

In this study, explicators of axiological text dominants of friend-foe groups are understood as the dispersion of pronouns of the I-we and you-they groups — that is, all classes of pronouns in direct and indirect cases are calculated across relevant groups [Stepanenko A.A., 2017: 17–25].

The thesaurus level is the hardest to formalize. While it is possible to create physical explication of the author's thesaurus [Bessmertny I.A., Nugumanova A.B., 2012: 125–130], it is still very difficult to identify how its lexemes "form up an orderly, fairly strict hierarchical system which reflects to some (indirect) extent the world's structure" [Karaulov Yu. N., 2010: 52]. This level is represented by the least number of parameters (three standard stylometric algorithms and one authentic rule) since the idea is not simply to formalize certain language personality elements for computer representation but also to make the resulting model interpretable.

A language personality's pragmaticon (a set of strategies and tactics, as well as means of their implementation that serve to achieve a speaker's

communicative purposes during communication) is formalized by the following set of parameters: parenthetic words and constructions expressing the subjective modality; purposive, intensifying and comparative locutions representing to what extent the author has mastered the written speech competencies and associated communicative strategies and tactics; syntactic clusters which give an idea, in particular, on the author's preferences regarding functional and stylistic association of the text; comparative, subordinate, one-member verb sentences expressing the functional type of narration; presence/absence and types of address as a contact establishing element. A total of 10 standard stylometric (searching for text statistics) algorithms and 32 unique rules were used.

It is not the pragmaticon units themselves ("communicative environment: domains, situations, roles" [Karaulov Yu. N., 2010: 61]) but indirect representatives of these units, components of the syntactic level that are assigned for the said level in the model. Therefore, in particular, the developed algorithm is not implementable without as an expert's judgment. That is, the author's competencies and aptitudes should be reproduced at the pragmatic level from the resulting statistical/syntactic information through interpretation. Let's take Sergei Dovlatov's collected stories "Nashi" to illustrate this process. Using the KhoRom software, we can extract 171 parenthetical constructions, a vast majority of which are conjunctive parenthetical constructions (krome togo, bolee togo, znachit etc. [except, moreover, hence] that create anaphoric linkages in the text. Thus, Dovlatov implements a competency of producing a coherent text, "aptitude of associating intentions, motives, planned meanings with the ways of their objectivation in the text". The identified value of parameters also allows to assert that the emotional charge of the speech ("aptitude of using stylistic means of this or another sublanguage") is largely produced by constructions different from parenthetical elements. The imagery becomes a major technique to create emotion in the text as proved by a comparison of syntactic complicators: the text has much more comparative than purposive phrases, their relative frequency of occurrence being 2669.85 against 715.14.

To analyze the syntactic structures, we introduced the rules based on POS tagging and on the types of syntactic relations found in the sentence [Paducheva E.B., 1974] and grammatical constructions implemented by its components. For instance, to identify parenthetical words, the formalized rule (search algorithm) will look as follows:

a vocabulary of all possible parenthetical words in Russian is created for computer-assisted representation;

a grammatical punctuation rule is assigned to identify parenthetical constructions rather than those homonymous to them:

1) __, Prnt,__

2) <start of sentence> Prnt,

where Prnt is any part of speech; __ — some part of the sentence while <start of sentence > marks the beginning of the sentence.

A search for one-member verb sentences — for example, definite personal ones — follows this algorithm:

+ V, 1per / 2per, sg / pl, praes / fut, indic

+ V, sg / pl, imper

3) — N / SPRO, nom, sg / pl

4) — NUM, nomn _+ N в gen/ gen2, pl

5) — many/few/several/some/considerable _ + N in gen/ gen2, pl.

The rule to search for purposive constructions is based on the semantic slot concept [Paducheva E.B., 1974: 44] and the grammar of prepositional constructions with double prepositions. Compound prepositions such as s tselyu/iz rascheta [for the purpose of/with a view to] will require an infinitive (as semantic slot condition) to have a purposive phrase, so the formalized rule to search for such constructions will look as follows: s tselyu/iz rascheta + INF where INF designates an infinitive.

Once all word structure-related parameters are retrieved, the ipm (instance per million) calculation is carried out. For syntactic parameters, the number of each parameter is divided by the number of sentences in the text. Designing a rule for automatic search of structures of the verbal semantic and motivational levels (those chosen for this study) is relatively simple. The resulting accuracy is high, with F-measure for all parameters varying from 0.89 to 1.

The output delivered by the algorithm are values of the Pearson correlation coefficient, linear regression (where determination coefficient should be assessed), Student's t-criterion for models of both compared texts, as well as the metrics of each parameter of the two texts to prove or refute H_0 hypothesis that both were authored by the same person.

Importantly, this module is not the final step in the developed methodology. As was said before, the text statistics need to be interpreted. Whereas a correlation coefficient of more than 65 percent is believed to be significant for the traditional mathematical statistics, it should be more than 86 percent for a software before we can assume the models are similar

[Radbil T.B., Markina M.V., 2019]. It is on purpose that the software does not generate the result in the form two compared texts are authored by the same person/two compared texts are authored by different persons since under the developed methodology the final attribution decision is to be made by an expert based, in particular, on statistical data (using checklist tables that was created on the basis of research findings, see Table 1) and his own investigative experience.

To construct such tables, the authors used text collections (see paragraph 3 of this paper for description), with 40 percent of texts in each analyzed through the use of the KhoRom resource in accordance with the patterns Author A = Author B (both texts were authored by the same person) and Author A ≠ Author B (texts were authored by different persons) in an equal or almost equal proportion (20 percent to 20 percent) to observe the statistical "behavior" in different instances. Based on the findings, checklist tables were constructed for each genre (non-genre prose fiction, web fiction, web journalism, entertainment journalism, corporate correspondence).

The methodology's performance was assessed from two perspectives: on the one hand, the resulting models of language personalities were considered from the viewpoint of theoretical assessment [Bloomfield L., 1926: 153–164]; [Hjelmslev L., 2005]; [Losev A.F., 2004]; [Apresyan Yu. D., 1966]; [Shtoff V., 1966]; [Revzin I.I., 1977]; [Belousov K.I., 2010: 94-97] etc., along with a set of criteria for indentifying the type of linguistic models (speech activity models, research models, meta-models etc.).

Thus, it could be asserted from a theoretical perspective that an integrative attribution model which includes parameters of three language levels quantitatively objectified and qualitatively assessed by an expert provides a relatively complete, comprehensive and at the same time objective imitation of the original. The point is that the resulting pool of parameters can reflect the information sufficient and necessary for author identification (completeness); the model structure extensively reproduces the author's original, individual style by incorporating the features of all three levels of the language personality (comprehensive imitation) while being devoid of the expert's personal assessments and judgments (objectivity).

All this allows the developed model to successfully solve practical problems of closed set identification (for a limited number of authors) through a pair-wise comparison of written texts of different lengths and genres.

[23] This probabilistic conclusion is due to the fact that under the developed methodology the authorship is to be attributed by the researcher.

Table 1. **Example of a checklist to assess the attribution model output**

Discourse type	Pearson correlation coefficient	Linear regression determination coefficient	Student's t-criterion (p-value)	Compared texts are likely[24] to be authored by the same person	Compared texts are unlikely to be authored by the same person	Comments
Web journalism	at 1.00	at 1.00	normally about 0.95; at least 0.93	+	—	P-value of Student's t-criterion is much less relevant for web journalism than for other discourses. If CC and DC values for web journalism reach 1, one can assume the compared texts were authored by the same person even if p-value of Student's t-criterion is not too high. On the other hand, p-value of Student's t-criterion may seem high but if the values of other metrics are low or not very high, one should adopt a comprehensive approach and analyze all information.
Web journalism	normally about 0.88 — 0.89	normally about 0.71 but can reach 0.77	can be both low (0.60) and relatively high (0.85)	—	+	
Web journalism	not very high at about 0.71	low: at about 0.50	can be very high: 0.98	—	+	

2.4. Validation of the attribution algorithm

The developed algorithm was tested and validated using the following text collections:

collection of prose fiction (10 texts in total) including texts by Sergey Dovlatov ("Nashi" [Our Folks], "Chemodan" [Suitcase], "Inostranka" [Foreigner], "Zapovednik" [Wildlife Sanctuary], "Zona: Zapisky Nadziratelya" [A Prison Camp Guard's Story], and Victor Astafiev ("Oberton" [Overtone],

"Posledniy poklon" [The Last Tribute], "Zvezdopad" [Shooting Star Shower], "Tak Khochetsya Zhit" [A Lust for Life]. The algorithm performed to 100 percent in terms of accuracy, precision and recall, with F-measure at 1[24];

collection of web fiction (Kniga Fanfikov web portal, 190 texts in total (https://ficbook.net/) including texts by 3 female and 4 male authors. The algorithm performed to 83 percent in terms of accuracy, precision and recall, with F-measure at 0.8;

collection of web journalism (The Village[25] newspaper, 600 texts in total) including texts by 3 female and 3 male authors. The algorithm performed to 100 percent in terms of accuracy, precision and recall, with F-measure at 1;

collection of entertainment journalism (Ya Plakal web portal, 600 texts in total) including texts by 3 female and 3 male authors. The algorithm performed to 40 percent in terms of accuracy, 0 percent in terms of precision and recall, with F-measure at 0;

collection of corporate Russian-language correspondence (218 texts in total) including texts by 2 female and 2 male authors. The algorithm performed to 83 percent in terms of accuracy, 67 percent in terms of precision and 100 percent in terms of recall, with F-measure at 0.8.

The authors explored a part of each text collection (about 60 percent) using the KhoRom tool in accordance with the patterns Author A = Author B and Author A ≠ Author B in an equal or almost equal proportion to search for true positive (TP), false positive (FP), false negative (FN) and true negative (TN) results of the algorithm's performance. The findings were presented in tables of the following form (Table 2):

Thus, where for the paired texts by A. Yakovlev "Podstavnye znakomstva" — A. Yakovlev "Kak vstrechayut Novy God v platzkarte, samolyote y na trasse" the KhoRom algorithm delivers the following statistics: Pearson correlation coefficient 1; linear regression determination coefficient 1; Student's t-criterion: p-value 0.94, an expert using a checklist table (Table 1) will conclude that "the compared texts were probably authored by the same person". This conclusion is true to the reality which means that the TP (true positive) column should be selected in Table 2.

As a result of analysis, conclusions were drawn and the following results obtained: the methodology could be used for attributing texts of different dis-

[24] Hereinafter the values of the metrics are specified in connection with interpretation of statistical data through the use of methodological recommendations and checklist tables developed for analytical purposes.

[25] Blocked in Russia.

Table 2. **Calculation of estimates to determine the algorithm's performance**

	Text pairs	TP	FN	FP	TN
1	A. Yakovlev: "*Podstavniye Znakomstva*" [Fake acquaintances] — A. Yakovlev "*Kak vstrechayut Novy God v platzkarte, samolyote y na trasse*" [Celebrating the New Year on the train, plane and road] (texts of the same genre by the same male author)	+	—	—	—
2	O. Karasyova: "*Gde deshevle zimovat — na Bali ily Shri-Lanke*" [The cheapest place to stay in winter: Bali versus Sri-Lanka] — O. Karasyova: "*Na chto zhivut zhurnalisty federalnykh kanalov*" [How the journalists of the federal channels make their living] (texts of the same genre by the same female author)	+	—	—	—
3	A. Yakovlev: "*Luchshye sovetskiye mozaiky v Moskve*" [The best Soviet-time mosaics in Moscow] — K. Rukov: "*Vyzhivut tolko spekulyanty: kak russky treider zarabotal million na obvale amerikanskoy birzhy*" [Only speculators will survive: how a Russian trader made a million on a U.S. stock market crash] (texts of the same genre (subject is disregarded) by different male authors)	—	—	—	+
4	O. Karasyova: "*Kak seitchas poyekhat na dachu*" [Going to one's country house right now] — A. Dergachyova: "*Rabochiye snova opustoshayut zapasy bobrov na Yauze*" [Workers destroy beavers' cache in the Yauza River again] (texts of the same genre (subject is disregarded) by different female authors)	—	—	—	+
etc.					

courses, given correct parameterization of models and correct interpretation of statistics for each text. In the course of the study, it was established that:

Student's t-statistics is the most informative for prose fiction discourse (both for established and pulp fiction authors);

stylo-statistics sets are non-informative for modern fiction texts since, as evidenced by experimental data, values of stylo-statistical parameters are closely related for all texts under study;

to identify the author of a journalistic text (in order to acknowledge H_0 hypothesis as true) the values of correlation and determination coefficients

should reach 1 (the need for these values to be that high is explained by the length and specific features of such texts). Importantly, it should be admitted that t-statistics — being the most informative for prose fiction texts — is much less relevant to the journalistic discourse. As regards gender differentiation of texts, it is noteworthy that "female" journalistic texts correlate more with other "female" texts which is equally true for "male" texts; the largest correlation differences are observed in individual styles of language personalities of different genders;

short text messages — corporate correspondence, Internet comments — require a representative sample of texts totaling at least 500 words. A limitation of 100 words suggested by C.M. Vul in his time and persisting in forensic authorship attribution to this day [Rubtsova I.I., Yermloayeva E.I., Bezrukova M.Yu. et al., 2007] as a length required to identify an author should be increased when statistical data is added to the analysis. For better handling of such texts, more parameters are currently being developed to construct idiostyle models as representations of language personality of the author since they are linked with the so-called digital handwriting style:

graphical liturative;

graphical hybridization;

playing upon archaic affixes;

using capitalized text elements;

emoticons and other graphical symbols expressing emotion of speech;

texts of different genres can also be validly examined using the developed integrative methodology (for instance, an electronic message can be compared with a feature article): the algorithms performs to 83, 67 and 100 percent in terms of accuracy, precision and recall, respectively, with F-measure at 0.8.

The methodology maximizes the value of idiostyle models rather than output data of an automatic algorithm. These models created as representation of authors' language personalities are understandable, simple, easily interpretable by experts, on the one hand, and provide a sufficiently complete and adequate imitation of the original, on the other hand.

The functionality of the algorithm in question and developed web resource is much wider than the capabilities originally built therein. The methodology can be used not only to solve identification problems of attribution linguistics but also to explore language personalities of writers, journalists, politicians etc. in diagnosing the language personality of specif-

ic individuals to address psycholinguistic and psychological problems, explore the generalized language personality of a given social group, subculture etc. to solve sociolinguistic and social science problems. Importantly, when the developed methodology is applied to any of the above cases, the model of a language personality will correspond to the theoretical principles of completeness, simplicity, adequacy, technically accurate and objective description of the original; it will be explanatory, communicative and interpretable.

3. Conclusions

Thus, it should be asserted that the integrative methodology combining the approaches of interpretative and cognitive linguistics with traditional stylometry is undoubtedly effective. The integrative approach seems to be the most appropriate basis for development of forensic investigation in Russia for a number of reasons: peculiarities of the regulatory framework in Russia; strong national tradition of interpretative linguistics; inadequacy of all known fully automatic methods of text attribution for forensic purposes (in terms of accuracy).

Importantly, under the proposed approach experts are not expected to do the interpretative part of the analysis themselves since the identification criteria can be assigned automatically while the process can be automated without prior manual text pre-processing and without using syntactic parsers. This feature is useful for developing a software prototype applicable, in particular, to problems of forensic linguistics as experts in authorship attribution do not always possess the required knowledge of corpus linguistics, statistics etc. The integration of all analytical modules in one software interface will allow to partially or probably fully automate the attribution analysis.

References

1. Apresyan Yu.D. (1966) *Ideas and methods of modern structural linguistics*. Moscow: Nauka, 302 p. (in Russ.)

2. Bacciu A., Morgia M. et al. (2019) Cross-domain authorship attribution combining instance-based and profile-based features. Notebook for PAN at CLEF 2019. Available at: http://ceur-ws.org/Vol2380/paper_220.pdf (accessed: 05.07.2020)

3. Baranov A.N. (2001) Introduction to Applied Linguistics. Manual. Moscow: Editorial URSS, 360 p. (in Russ.)

4. Batura T.V. (2012) Formal Ways of text authorship identification. *Vestnik Novosibirskogo gosudarstvennogo universiteta. Informatcionnye tehnologii*=Journal of Novosibirsk State University. Information Technology, vol. 2, no. 4, pp. 81–94 (in Russ.)

5. Belousov K.I. (2010) Linguistic Models and Language Reality Modeling Issues. *Vestnik Orenburgskogo gosudarstvennogo universiteta*=Journal of Orenburg State University, no. 11, pp. 94–97 (in Russ.)

6. Bessmertny I.A., Nugumanova A.B. (2012) Automatic Thesaurus Building Method Based on Statistical Processing of Texts in the Natural Language. *Izvestia Tomskogo gosudarstvennogo politekhnicheskogo universiteta*=Proceedings of Tomsk State Polytechnical University, no. 5, pp. 125–130 (in Russ.)

7. Bloch B. (1948) A set of postulates for phonemic analysis. *Language*, vol. 24, no. 1, pp. 3–46.

8. Bloomfield L. (1926) A set of postulates for the science of language. *Language*, vol. 2, no. 2, pp. 153–164.

9. Campbell L. (1867) *The Sophisties and Polilicus of Plato*. Oxford: Clarendon Press, 170 p.

10. Coulthard M. (2004) Author identification, idiolect, and linguistic uniqueness. *Applied Linguistics*, vol. 24, no. 4, pp. 431–447.

11. Custódio J., Paraboni I. (2018) EACH-USP Ensemble Cross-Domain Authorship Attribution. Notebook for PAN at CLEF 2018. Available at: http://ceur-ws. org/Vol-2125/paper_76.pdf (accessed: 05.07.2020)

12. Encyclopedia of Forensic Science (1999) T.B. Averyanova (ed.). Moscow: Prospekt, 442 p. (in Russ.)

13. Galyashina E.I., Yermolova E.I. (2005) Linguo-forensic tools for authorship attribution of written and oral texts. Papers of the International Research Conference. Moscow, pp. 20–22 (in Russ.)

14. Gomzin A. et al. (2018) Detection of author's educational level and age based on comments analysis. Paper presented at Dialogue, Moscow, 30 May–2 June 2018. Available at: URL: http://www.dialog-21.ru/media/4279/gomzin_turdakov.pdf (2018) (accessed: 05.07.2020) (in Russ.)

15. Goroshko E.I. (2003) Forensic authorship attribution: gender identification of the author of a document. Theory and practice of forensic investigation and science. *Pravo*, no. 3, pp. 221–226 (in Russ.)

16. Hjelmslev L. (2005) *Prolegomena to a theory of language*. Moscow: Editorial URSS, 243 p. (in Russ.)

17. Juola P. (2006) Authorship Attribution. *Foundations and Trends in Information Retrieval*, vol. 1, no. 3, pp. 233–334.

18. Ionova S.V., Ogorelkov I.V. (2020) Gender-based Individual Speech Diagnostics in Authorship Attribution: Quantitative Approach. *Vestnik*

Volgogradskogo gosudarstvennogo universiteta. Linguistika=Journal of Volgograd State University. Linguistics, vol. 19, no. 1, pp. 115–127. DOI:https://doi.org/10.15688/jvolsu2.2020.1.10 (in Russ.)

20. Karaulov Yu. N. (1987) *Russian Language and Language Personality*. Moscow: Nauka, 264 p. (in Russ.)

21. Khmelyov D.V. (2002) Linguo-analyzer. E-resource. Available at: URL: http://www.rusf.ru/books/analysis/ (accessed: 16.11.2017) (in Russ.)

22. Khomenko A., Baranova Yu., Romanov A., Zadvornov K. (2021) The Linguistic modeling as a basis for creating authorship attribution software. Computational linguistics and intellectual technologies. Proceedings of the International Conference "Dialogue 2021" Moscow. Available at: URL: http://www.dialog-21.ru/media/5315/khomenkoaplusetal048.pdf (accessed: 23.06.2021) (in Russ.)

23. Komissarov A.Yu. (2000) Forensic Investigation of Written Speech: Manual. Moscow: Forensic Agency of the Interior Ministry of the Russian Federation, 126 p. (in Russ.)

24. Koppel M., Schler J. (2003) Exploiting Stylistic Idiosyncrasies for Authorship Attribution. Proceedings of IJCAI'03 Workshop on Computational Approaches to Style Analysis and Synthesis, vol. 69, pp. 72–80.

25. Korobov M. (2015) Morphological analyzer and generator for Russian and Ukrainian languages. In: Khachay M.Y., Konstantinova N.A. (eds.). AIST 2015. CCIS, vol. 542, pp. 320–332. Available at: https://doi.org/10.1007/978-3-319-26123-2_31 (accessed: 05.07.2020) (in Russ.)

26. Leonard R., Ford J., Christensen T. (2017) Forensic linguistics: applying the science of linguistics to the issues of the law. *Hofstra Law Review*, vol. 45, pp. 881–897.

27. Linguistics of Constructions (2010) E.V. Rakhilina (ed.). Moscow: Azbukovnik Publishing, 584 p. (in Russ.)

28. Litvinova T.A. (2019) Idiolect as Object of Corpus Idiolectology: Towards a New Field in Linguistics. *Vestnik Novgorodskogo gosudarstvennogo universiteta imeni Yaroslava Mudrogo*=Bulletin of the Yaroslav Mudriy Novgorod State University, no. 7, pp. 1–5 (in Russ.)

29. Litvinova T., Rangel F. et al. (2017) Overview of the Rus Profiling PAN at FIRE Track on Cross-genre Gender Identification in Russian. Working notes of FIRE 2017. Forum for Information Retrieval Evaluation. Bangalore, pp. 1–7. Available at: URL: http://ceur-ws.org/Vol-2036/T1-1.pdf (accessed: 05.07.2019) (in Russ.)

30. Litvinova T.A., Gromova A.V. (2020) The Use of Computer Technologies for Forensic Authorship Attribution: Issues and Prospects. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Lingvistika*=Journal of Volgograd State University. Linguistics, vol. 19, no. 1, pp. 77–88. DOI: https://doi.org/10.15688/jvolsu2.2020.1.7 (in Russ.)

31. Litvinova T., Sboev A., Panicheva P. (2018) Profiling the age of Russian bloggers. Proceedings of the 7th International Conference, AINL 2018. Saint Petersburg, pp. 167–177 (in Russ.)

32. Losev A.F. (2004) Introduction to the General Theory of Linguistic Models. Moscow: Editorial URSS, 293 p. (in Russ.)

33. Marusenko M.A. (1990) The use of image recognition methods for attribution of anonymous and pseudonymous literary texts. Leningrad: University, 1990. 164 p. (in Russ.)

34. Marusenko M.A. (2003) Attribution of anonymous and pseudonymous texts as a standard image recognition problem. *Istoriographiya y istochnikovedeniye otechestvennoy istorii*=Historiography and Research of Sources of National History, no. 3, pp. 18–22 (in Russ.)

35. McMenamin G. (2002) *Forensic linguistics: advances in forensic stylistics*. London: Routledge, 361 p.

36. Murauer B., Tschuggnall M., Specht G. (2018) Dynamic Parameter Search for Cross-Domain Authorship Attribution. Notebook for PAN at CLEF 2018. Available at: http://ceur-ws.org/Vol-2125/paper_84.pdf (accessed: 05.07.2020)

37. Muttenthaler L., Lucas G., Amann J. (2019) Authorship Attribution in Fan-Fictional Texts given variable length Character and Word N-Grams. Notebook for PAN at CLEF 2019. Available at: http://ceur-ws.org/Vol-2380/paper_49.pdf (accessed: 05.07.2020)

38. Paducheva E.B. (1974) *On semantics of syntax*. Moscow: Nauka, 291 p. (in Russ.)

39. Radbil T.B., Markina M.V. (2019) Probability Statistical Models in Attribution of Texts by Russian Language Authors. *Politicheskaya Lingvistika*=Political Linguistics, no. 2, pp. 156–166 (in Russ.)

40. Revzin I.I. (1977) *Modern Structural Linguistics: Issues and Methods*. Moscow: Nauka, 263 p. (in Russ.)

41. Rodionova E.S. (2008a) Linguistic Methods of Attribution and Dating of Literary Texts: towards Corneille-Moliere Problem. Candidate of Philological Sciences Summary. Saint Petersburg, 25 p. (in Russ.)

42. Rodionova E.S. (2008b) Methods of literary text attribution. In: Structural and applied linguistics: inter-university collection. A.S. Gerda (ed.). Saint Petersburg: University, 2008, pp. 118–127 (in Russ.)

43. Rogov A.A. et al. (2019) Software support for solving text attribution problems. *Programmnaya Inzheneriya*=Programming Engineering, no. 5, pp. 234–240 (in Russ.)

44. Romanov A.S. (2010) Methodology and Software Package for Identification of Authors of Unknown Texts. Candidate of Engineering Sciences Summary. Tomsk, 26 p. (in Russ.)

45. Romanov A.S., Kurtukova A., Fedotova A. et al. (2021) Authorship Identification of a Russian-Language Text Using Support Vector Machine and Deep Neural Networks. *Future Internet*, vol. 13, issue 3, pp. 1–16.

46. Rubtsova I.I., Yermolayeva E.I., Bezrukova A.I. et al. (2007) Comprehensive methodology of authorship attribution: methodological recommendations. Moscow: Forensic Agency of the Ministry of Interior, 192 p. (in Russ.)

47. Russian Grammar Rules: Collected works (2005) N. Yu. Shvedov (ed.). Moscow: Nauka, 665 p. Available at: URL: http://rusgram.narod.ru/index.html. (in Russ.)

48. Shevelyov O. G. (2007) Methods of automatic classification of texts in the natural language: manual. Tomsk: TML-Press, 144 p. (in Russ.)

49. Shtoff V. (1966) *Modeling and philosophy.* Moscow: Nauka, 304 p. (in Russ.)

50. Shuy R. (2005) *Creating Language Crimes: How Law Enforcement Uses (and Misuses) Language*. N. Y.: Oxford University Press, 194 p.

51. Sidorov Yu.B. et al. (1999) Computer-assisted system for linguistic analysis of literary texts. In: Saint Petersburg Assembly of Young Researchers and Specialists. Abstracts of reports. Saint Petersburg: University Press, p. 66. (in Russ.)

52. Stamatatos E. (2017) Authorship attribution using text distortion. Proceedings of 15th Conference of the European Chapter of the Association for Computational Linguistics, Long Papers, pp. 1138–1149.

53. Stepanenko A.A. (2017) Gender attribution of computer network communication texts. *Vestnik Tomskogo gosudarstvennogo universiteta*=Journal of Tomsk State University, no. 5, pp. 17–25. DOI: 10.17223/15617793/415/3 (in Russ.)

54. Timashev A.N. (2007) Atributor: version 1.01: software description. Available at: URL: http://www.textology.ru/atr_resum.html (accessed: 01.02.2016) (in Russ.)

55. Vinogradov V.V. (1961) *The Authorship Problem and Theory of Styles*. Moscow: Goslitizdat, 614 p. (in Russ.)

56. Vul S.M. (2007) Forensic Authorship Identification: Methodological Basis. Guidebook. Kharkov: KhNIISE Press, 64 p. (in Russ.)

57. Wright D. (2017) Implementing word n-grams to identify authors and idiolects: a corpus approach to a forensic linguistic problem. *International Journal of Corpus Linguistics*, vol. 22, no. 2, pp. 212–241.

58. Zakharov V.N. et al. (2000) System Support Programme for Attribution of Articles Authored by F.M. Dostoevsky. *Trudy Petrozavodskogo gosudarstvennogo universiteta*=Research Works of the Petrozavodsk

State University. Applied Mathematics and Information Technology Series, issue 9, pp. 113–122 (in Russ.)

59. Zakharov V.N., Khokhlova M.V. (2008) The Statistical Method for Identification of Collocations. Language Engineering in Search of Meanings. Collection of reports to the conference workshop "Web-Based Linguistic Information Technologies". 11th All-Russia Joint Conference "Internet and Modern Society". Saint Petersburg: University, 2008, pp. 40–54 (in Russ.)

Information about the authors:

T.B. Romanova — Professor, Doctor of Sciences (Philology).

A.Yu. Khomenko — Senior Lecturer, Candidate of Sciences (Philology), expert.

The article was submitted to the editorial office 17.01.2022; approved after reviewing 21.03.2022; accepted for publication 15.04.2022.

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

Comment

Review
УДК: 347
DOI:10.17323/2713-2749.2022.2.116.140

Key Issues in the Intellectual Property Court's Presidium Rulings

Natalia Igorevna Kapyrina[1], Maria Alexandrovna Kolzdorf[2]

[1] MGIMO University, 76 Prospekt Vernadskogo, Moscow 119454, Russian Federation, n.kapy rina@ my.mgimo.ru, ORCID: 0000-0003-1276-1600, Researcher ID: AAQ-3784-2021

[2] National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russian Federation, Researcher ID: AAI-1625-2019, mkolzdorf@hse.ru, ORCID:0000-0003-3227-3348, Researcher ID: AAI-1625-2019

Abstract

The comment reviews key positions in the rulings of the Presidium of the Russian Intellectual Property Court (IPC) issued in December 2021 and January 2022. This Chamber hears cassation appeals against the decisions of the IPC first instance and deals primarily, but not only, with matters of registration and validity of industrial property rights. Therefore, this review predominantly covers substantive requirements for patent and trademark protection, as well as procedural issues both in the administrative adjudicating mechanism at the Patent office (Rospatent) and at the IPC itself. The current review encompasses a variety of topics related to trademark law: signs that are contrary to the public interest, signs conflicting with an earlier trademark or an appellation of origin, signs using a geographical name, deceptive signs, the comparison of signs, trademark revocation for lack of use, unfair competition, procedural challenges, etc. The review further considers one patent case, in which the IPC Presidium resolved the issue of establishing priority date for a divisional application for a utility model derived from an application initially filed for an invention.

Keywords

Russia, case-Law, trademarks, revocation, similarity, unfair competition, public interest, appellations of origin, utility model, patent.

For citation: Kapyrina N.I., Kolzdorf M.A. (2022) Key Issues in the Intellectual Property Court's Presidium Rulings. *Legal Issues in the Digital Age*, vol. 3, no. 2, pp. 116–140. DOI:10.17323/2713-2749.2022.2.116.140

I. Trademarks

1. Traditional Crafts as Signs Contrary to the Public Interest

Registering a graphical sign that alludes to the style of a popular artistic handicraft is contrary to public interest.

Ruling of the IPC Presidium dated 24 January 2022 in case No. SIP-637/2021

The Contested Sign

Rospatent refused to register a trademark for goods and services in ICGS Classes 5, 32 and 35 because the registration of such a sign was contrary to the public interest (Article 1483.3.2 of the Civil Code of the Russian Federation; hereinafter: CC RF) and also because the sign might mislead consumers as regards the place of manufacture (CC RF, Article 1483.3.1).

Following the applicant's appeal Rospatent upheld the registration refusal on the grounds of CC RF Article 1483.3.2. The applicant contested that decision before the IPC, but both the first instance court and the cassation instance court upheld the IP office's finding that the sign was contrary to the public interest.

Both Rospatent and the first instance court established that the lower part of the image reproduced an ornament that was characteristic of the Gzhel popular handicraft, which is recognised as part of the Russian peoples' cultural heritage and a form of cultural expression, both protected and registered under the Federal Law No. 7-FZ On Popular Artistic Handicrafts (hereinafter referred to as 'Handicrafts Law'). The applicant disagreed with the findings and pointed out that the upper part of the sign contained an

image of mountains and a stylised bird while its lower part included touches of red and brown colours — neither feature being typical of Gzhel white and blue porcelain. Nevertheless, the first instance court concluded the consumer's perception of the contested image would evoke precisely Gzhel ornaments as the sign's lower part included a figurative element possessing the typical artistic features of that handicraft. The court also observed that the sign's lower part dominated the upper part, and the consumer's first impression of the sign would definitely lead to associate the whole sign with the popular artistic handicraft.

The IPC Presidium upheld the first instance court's conclusions. It explained that, in this case, contradiction to public interest consisted in the fact that the registration of the trademark would impose restrictions, that are not prescribed by law, on third parties. It will be particularly the case of popular handicraft makers, referred to in Article 5 of the Handicrafts Law, who will not be able to use specific interpretations of the Gzhel style.

The cassation instance court also dismissed the applicant's argument that many manufacturers used such figurative elements, for it was the contested sign that was being checked for validity in this case. The judges noted that, conversely, that argument confirmed that the contested sign failed to meet the requirements of CC RF Article 1483.3.2.

2. Geographical names in Trademarks

As a sign is assessed for validity, any findings on its possible association with a specific geographic site should be based on whether the target group of consumers may associate that very site with the goods and services claimed in the application, rather than how well its country or location is known as the goods' place of manufacture.

Validity of the contested sign should be assessed with respect to each good or service in question, but the findings may apply to groups of those — provided that good reasons are given for grouping them together.

Ruling of the IPC Presidium dated 24 January 2022 in case No. SIP-762/2021

The Contested Sign

Rospatent refused to register a combined sign containing 'Окинава' (Okinawa) verbal element as a trademark for a broad range of goods and services — mainly foodstuffs, advertising, and goods delivery. The IP of-

fice's findings were based on the sign's non-conformity with CC RF Articles 1483.1.3 (descriptive signs) and 1483.3.1 (deceptive signs). Rospatent proceeded from the fact that Okinawa was known to the Russian consumer as a Japanese island and that Japan was a manufacturer and global exporter of various foodstuffs; consequently, the sign described the goods by reference to their place of manufacture. The IP office also pointed out that the applicant was a Russian citizen based in the city of Kazan, so the contested sign could mislead the consumer as to the place of manufacture of the goods claimed in the application. After his appeal at Rospatent was rejected, the applicant referred to the IPC. The IPC decided to allow the applicant's claims. Furthermore the cassation appeal lodged by Rospatent to the IPC Presidium was dismissed.

The IPC Presidium recalled that, where a geographical name is used in a sign, in order to find whether the sign conforms to CC RF Article 1483.1.3, one must establish not only whether the geographical object exists at all but also whether it is known to the target group of consumers and whether an average or ordinary consumer can perceive the geographical term as the specific good's place of manufacture. The last finding should be based on whether consumers feel any association between a specific good item and a specific sign.

In this case, any findings about possible association should have been based on whether the target consumer group could associate precisely the island of Okinawa with the corresponding goods and services, rather than on the general renown of Japan as a goods manufacturer. In other words, the task was to find whether it could reasonably be assumed that the 'Okinawa' verbal element designated the origin of the contested goods and services to the target consumer group.

To refute these findings of the first instance court, Rospatent, in its cassation appeal, argued particularly that the court's methodological approach to that matter departed from the international practice and, in particular, from the Trademark Examination Guidelines of the European Union Intellectual Property Office (hereinafter referred to as 'EUIPO Examination Guidelines'). The IPC Presidium disagreed with Rospatent's position and explained that the interpretation of the rule in CC RF Article 1483.1.3 by the first instance court was in line with the content of the EUIPO Examination Guidelines.

Firstly, Para 2.6.2 of Section 4, Chapter 4, Part B of the EUIPO Examination Guidelines cited by Rospatent points out that the registration of

geographical names as trademarks is not possible where such a geographical name is either (1) already famous, or (2) is known for the category of goods/services concerned, and is therefore (1) associated with those goods or services in the mind of the relevant class of persons, or (2) it is reasonable to assume that the term may, in view of the relevant public, designate the geographical origin of the category of goods and/or services concerned. When assessing a specific geographical name (rather than the country in which the site in question is located), a two-step test should be carried out:

Establish whether the relevant public understands the specific term as a geographical name (the general rule permits the registration of geographical names unknown to a reasonably informed consumer who is not an expert in geography);

Establish whether the term designates a place that the relevant public currently associates with the goods or services claimed or whether it is reasonable to assume that it will associate with those goods or services in the future, or whether such a name may, in the mind of the relevant public, designate the geographical origin of that category of goods or services (i.e., the test must be performed in respect of specific goods and services in question).

The EUIPO Examination Guidelines also expressly state that registration refusal cannot be based solely on the argument that the goods can theoretically be produced at that location.

Secondly, as regards the SUEDTIROL case cited in the cassation appeal, the IPC Presidium indicated that Rospatent had failed to accurately reproduce the EU General Court's position in stating that 'to establish association between a geographical name and goods and services, it is sufficient to establish that the goods and services in question can be made in a region with a certain level of economic development in principle'. The IPC Presidium stated that in the above quotation Rospatent had replaced the expression, 'such as those [claimed in the patent application]' with the words 'claimed in the patent application', meaning the concrete services claimed rather than a class of these — and failed to take into account what kind of services were actually implied in the example.

Moreover, in the case in question, the association was established on the basis of evidence submitted and on the actual circumstances. Thus, it follows from the EU General Court's decision that it took into account the specificities of the region whose name (SUEDTIROL) was used as the claimed sign, and the existence of businesses providing the contest-

ed services in the region (Para 41–44 of the General Court judgement in case T-11/15 of 20.07.2016). On the other hand, the EUIPO Examination Guidelines cite examples of possible registration, such as HOLLYWOOD for Class 30 goods and GREENLAND for fresh vegetables and fruit.

The latter fact also refutes Rospatent's argument that a special approach should be applied to foodstuffs, one allegedly existing in world practice and precluding the existence of trademarks that employ geographical terms. In adopting the contested decision, Rospatent proceeded from the following:

Russian consumers know about the island of Okinawa because the world-wide web abounds in links to information in Russian language about that geographic site; and

Japan produces various foods and beverages, such as soybean sauce, miso, soybean milk, tofu, and sake, and exports those foods and beverages to various countries, such as China, Thailand, South Korea, the USA, Mexico, Canada, and Australia, which shows that Class 29, 30, 31, and 32 goods are promoted in and delivered to many parts of the world.

The IPC Presidium found such approach unacceptable. The Court held that the first instance court had been correct in pointing out that 'the fact that Japan is known as the place of manufacture of a range of foodstuffs is not sufficient to make a conclusion that the Japanese island of Okinawa is known as a place of manufacture of all the goods listed in the application. Given the existing diversity of foodstuffs and various conditions for making them (natural, climatic, and others), one region cannot be known as the origin of all foodstuff.'

In respect of Rospatent's argument that it could not be reasonably required to assess the protectability of a contested sign for any claimed good or service, the IPC Presidium recalled that what mattered was whether Rospatent's actions were legal, and not reasonable. In reviewing an application, examiners focus on the possibility of registering the contested sign in respect of each designated good (from those included in the application). As the appeal is assessed, the purpose is to check the legality of the examiner's decision in respect of each designated good (out of those included in the appeal). When the case is taken up by court, the object of the dispute is to check the legality of the Rospatent decision in respect of each designated good (out of those included in the appeal filed with the court).

On the other hand, the IPC Presidium does not rule out the possibility of making consolidated conclusions on groups of goods (rather than individual goods items) or market sectors, but only if good reasons are given for

grouping the goods items together to assess the probable perception of the contested sign by target consumer audiences. And, finally, the Presidium upheld the first instance court's finding that consumers could not be possibly misled in the sense of CC RF Article 1483.3.1. It noted that the court had used a correct methodology and properly concluded that, in violation of the rules of law and methodological recommendations, Rospatent's decision had failed to analyse the probability of false association in respect of the list of goods and services listed in the application.

3. Multiple Companies in the Market Using the Same Word Sign and Consumers' Deceit

If there are two entities using the same word sign in a certain market, it is not enough to find associations with only one of them for concluding that consumers can be misled.

Ruling of the IPC Presidium Resolution dated 24 December 2021 in Case No. SIP-387/2021

Rospatent refused to register a combined sign including the 'WABI' verbal element as a trademark for ICGS Class 9 goods and Class 35, 38, 42 services. The office concluded that the sign was contrary to the public interest (CC RF Article 1483.3.1) and contained an element, which could mislead the consumer in respect of the goods and services listed in the application (CC RF Article 1483.3.2).

After its appeal was dismissed by the administrative body, the applicant lodged an appeal at the IPC. The first instance decision, later upheld by the cassation instance court, found the Rospatent decision invalid and obliged the office to re-consider the appeal.

Rospatent's cassation appeal focused on the non-conformity of the first instance decision to CC RF Article 1483.3.2 only. It should however be noted that the first instance court dismissed Rospatent's conclusion that the contested sign included the name of the Wabi cryptocurrency and was thus contrary to the public interest. In sum the IP office had proceeded from the Bank of Russia warning that cryptocurrencies could be used in criminal activities. The first instance court stated in its decision that Rospatent had given no justifications as to how the registration of the sign for identifying the designated goods and services will be perceived as contrary to the public interest. That conclusion by Rospatent also deviated from the existing practice of registering signs with names of cryptocurrencies, particularly for Class 36 financial services.

In respect of the non-conformity of the IPC judgement to the provisions of CC RF Article 1483.3.2, the IPC Presidium noted that this substantive rule codifies an absolute ground for refusal of a trademark registration and applies where the sign itself, due to its particular features, is false or misleading to the consumer. Signs that may mislead the consumer in respect of the goods manufacturer or service provider may include imitations of signs used for marking goods and/or services and well known to the consumers. In some cases, claimed signs imitate those that have not been registered as trademarks but are used by other businesses.

The Presidium observed that Rospatent's finding that the contested sign was deceptive for the consumer had resulted from the fact that its verbal element is used by the Chinese company Walimai (currently known as Taeltech). However, the first instance court established that the applicant had submitted documents evidencing the use of the same verbal element by the Coca-Cola company.

As the Presidium explained, when two foreign entities use the same sign in online trade, conclusions that the Russian consumers could have associated it with just one of the entities cannot be made on the basis of mere assumptions. Besides, Rospatent should have analysed the probability of the emergence of associative links with each of the companies. The Presidium also noted that the contested sign was a combination sign and included a figurative element. That was also to be taken into account in determining whether consumers in the Russian Federation associated that specific contested sign with any sign used by foreign entities, and with which one, if they did.

4. Challenging the Protection of Trademarks that Were Granted in Connection with the Accession of Crimea

Trademarks recognized as such under the legislation of the Russian Federation on the grounds of Article 13.1.1 of the Introductory Act to the CC RF may be contested in court if the exclusive right thereto has been acquired by an ineligible person (Article 13.1.16 of the Introductory Act).

Unlike the general procedure whereby mala fide acquisition of the exclusive right to a trademark is established pursuant to a separate claim, for trademarks recognised as such under Article 13.1 of the Introductory Act the recognition of mala fide acquisition is not a separate claim but only a ground for another claim based on Article 13.1.16 of the Introductory Act.

Ruling of the IPC Presidium dated 22 December 2021 in Case No. SIP-581/2019

The SHUSTOV (ШУСТОВ) trademark was registered after OOO Krymsky Vinny Dom (Crimean Wine House) applied on 15.03.2016 to have their exclusive right to a Ukrainian-certified (parent) trademark recognized in the territory of the Russian Federation.

The Shustov Trade House contested the legal protection granted to the above trademark before Rospatent, stating that its registration did not conform to Article 13.1.1 of Federal Law No. 231-FZ 'On the Enactment of Title Four of the Civil Code of the Russian Federation' dated 18 December 2006 (hereinafter referred to as 'Introductory Act'). To justify their challenge, the applicant stated that as of 18.03.2014 (the day when the Republic of Crimea was admitted into, and new subjects formed in the Russian Federation) OOO Krymsky Vinny Dom had no right to the parent trademark. The company acquired the said right as late as 10 July 2014 from a foreign entity located outside the Republic of Crimea.

In view of the foregoing, the Shustov Trade House believed that the Crimean Wine House's exclusive right to the contested trademark could not be recognized in the territory of the Russian Federation, for on that date when the Republic of Crimea was admitted into the Russian Federation and new subjects formed in the Russian Federation, the exclusive right to the parent trademark belonged to a foreign entity whose standing executive body was not based in the territory of the Republic of Crimea. The Shustov Trade House also pointed out that the Crimean Winery's action to acquire the exclusive right to the contested trademark after 18 March 2014 and seek recognition thereof in the territory of the Russian Federation was actually abuse of right.

Rospatent decided to dismiss the challenge and to continue the legal protection of the contested trademark. Rospatent stated inter alia that it could not consider the Shustov Trade House's references to non-conformity of the registration of the contested trademark to Article 13.1.1 and 13.1.4 of the Introductory Act because CC RF Article 1512 provided for no such ground for an administrative challenge against registration.

The Shustov Trade House brought two claims before the IPC:

To find invalid the decision taken by Rospatent after considering the challenge, and

To find invalid the granting of legal protection to the contested trademark.

In this case, the regulation contained in Article 13.1.16 of the Introductory Act means that the claim for the invalidation of the legal protection

provided to the contested trademark constitutes a separate claim rather than a remedy sought by the Shustov Trade House (Article 201.4.3 of the Code of Commercial Procedure of the Russian Federation, hereafter: CCP); Article 13.1.16 of the Introductory Act stipulates that the recognition of the exclusive right to a trademark performed in violation of Parts 3 and 4 of Article 13.1 may be contested directly in court.

The first instance court accepted the modified claim lodged the following wording: 'To declare the actions related to the acquisition of the exclusive right to the trademark … an act of unfair competition and abuse of the respective right, and to terminate legal protection of the said trademark.' The owner pointed out that this modification infringed the rules of CC RF Article 49 as it altered both the claim's subject matter and ground at the same time. Disagreeing with that argument, the IPC Presidium noted that in this case both the subject matter and the ground of the claims brought had remained essentially unchanged.

In this case, the substantive claim consisted in a desire to have the legal protection of the contested trademark terminated.

Both initially and as modified, the claim was based on the fact, as alleged by the Shustov Trade House, that the Crimean Wine House had submitted improper documents to Rospatent to confirm that the former possessed the exclusive right to the parent trademark under Ukrainian legislation, in order to have it recognised under the legislation of the Russian Federation on the basis of Article 13.1.1 of the Introductory Act.

As noted in Para 171 of the resolution of the Plenum of the Supreme Court of the Russian Federation No. 10 dated 23 April 2019 "On Application of Title Four of the Civil Code of the Russian Federation" (hereafter — Resolution No. 10), provision of untruthful documents to Rospatent with the application for the registration of a trademark may indicate a mala fide action.

Trademarks recognized as such under the legislation of the Russian Federation on the grounds of Article 13.1.1 of the Introductory Act are specific in that they are may be contested directly in court if the exclusive right to them was acquired by an ineligible person (Article 13.1.16 of the Introductory Act).

If it is established that untruthful documents have been filed (i.e., mala fide action in the sense of Para. 171 of Resolution No. 10) to confirm that the person in question possesses the exclusive right by virtue of Article 13.1.1 of the Introductory Act, then the court will directly invalidate the legal protection to such a trademark.

Consequently, unlike the general procedure whereby mala fide acquisition of the exclusive right to a trademark is established pursuant to a separate claim, for trademarks recognised as such under Article 13.1 of the Introductory Act the recognition of mala fide acquisition is not a separate claim but only a ground for another claim based on Article 13.1.16 of the Introductory Act.

Thus, 'declaring any actions involved in the acquisition of exclusive rights to a trademark … an act of unfair competition and abuse of the respective right' only constitutes proper legal assessment of a claim to invalidate the legal protection provided to the contested trademark.

In this case, both unfair competition and the abuse of the right constitutes not a claim in itself but a legal ground for claiming the termination of the legal protection of the contested trademark on the ground of Article 13.1 of the Introductory Act.

5. Similarity between Signs

Due to consumers' cognitive capacities, in assessing the similarity between two signs experts need to identify and compare the elements that the consumer will remember best.

Ruling of the IPC Presidium dated 16 December 2021 in case No. SIP-499/2021

Contested sign

Earlier trademark

Rospatent refused to register a trademark, finding that the sign in the application failed to meet the requirements of Article 1483.1 (descriptive element) and 1483.6.2 (conflict with an earlier trademark) of the CC RF. Firstly, the realistic image of a dog included in the sign was a non-protectable element in respect of part of Class 31 goods ('live animals') as it characterises to the goods' type. Secondly, the sign was similar to the degree of confusion to a number of trademarks previously registered for similar goods. After the administrative appeal was dismissed, the applicant lodged an appeal at the IPC challenging the Rospatent decision in its second ground of dismissal only (likelihood of confusion). The first instance court's decision, later upheld by the IPC Presidium, dismissed the applicant's submission.

In the cassation appeal, the applicant challenged the first instance court's conclusion that the sign in question was similar to the degree of confusion with the opposed sign but did not argue against the court's findings that the goods were similar. The cassation court confirmed that the first instance court had correctly applied the methodology for establishing similarity as set out in Rospatent Decision No. 482 and Para 162 of the Resolution No. 10. The IPC Presidium stated that in assessing similarity of these signs, the first instance court proceeded on the basis that each of them depicted an animal (a realistic image of a dog and a stylised image of a cat and a dog) with a human hand above the animals. The position of the animal's head (looking up) and the image of the human hand that is about to pet the animal is the same on both images. The fact that there are differing elements cannot prove a complete lack of similarity between the signs at issue.

The IPC Presidium explained there was a reason why Para 162 referred to the need to establish similarity on the basis of strong elements in the first place.

Considering the fact consumer usually does not see two signs at the same time, one beside the other (unlike the court, Rospatent, and the representatives of the litigants), the elements that are remembered best must be identified. Since the consumer tends to forget the details, it makes no sense to take into account the distinction between the details alone. In the case at issue, there is clear similarity between the ideas implied in the signs submitted for comparison: the presence of an animal head in a particular similar posture and of the human hand in a particular similar position. This is the element that will leave the strongest impression, so this is what the first instance court took into account.

Considering that the appealing party did not challenge the first instance court's decision on the goods' high degree of similarity, the IPC Presidium ruled that the conclusion of the first instance court that the sign applied for registration did not meet the provisions of Article 1483.6.2 of the CC RF was justified.

6. Trademark revocation for non- use

While a clinical trial can be a reason for not using a trademark registered for pharmaceutical goods, the acts and events that were in the rightholder's sphere of influence and responsibility cannot be cited as obstacles independent of its will.

Ruling of the IPC Presidium dated 16 December 2021 in case No. SIP-58/2021

The Citomed company appealed to the IPC Presidium against the decision of the first-instance court revoking the company's trademark REGASTIM based on lack of use with respect to ICGS Class 5 goods (pharmaceutical goods).

The appellant did not challenge the court's conclusion that its trademark had not been used for a three-year period but it justified non-use by circumstances beyond its control. Citomed clarified that it was conducting a clinical trial necessary for the registration of the pharmaceutical product it was intending to launch under the contested trademark. Furthermore, the company indicated there was an obstacle allegedly preventing the registration of its product, namely the earlier registration of a pharmaceutical product named REGAST, made by the Pharmasintez company. The latter company initiated the revocation proceedings for the contested trademark. The first instance court concluded the trademark owner did not present any evidence showing that there were obstacles to the completion of the clinical trial within the time frame required. On the contrary, based on the case materials, the court established that, having obtained authorisation to conduct the trial, the trademark proprietor had not taken any active steps for several years to actually conduct this trial.

The IPC Presidium upheld the first instance court's decision noting that, while conducting a clinical trial can be a reason for a failure to put the trademark to use, the acts and events cited by Citomed were within its sphere of influence and responsibility so they could not be regarded as obstacles independent of its will. The IPC Presidium indicated that a similar legal approach was adopted in international practice (Judgment of the EU Court of Justice dated 03 July 2019 in case No. C-668/17P). With respect to the applicant's statement that the clinical trial was time-consuming and costly, the IPC Presidium clarified as follows: non-use of a trademark by the rightholder cannot be justified in circumstances where such lack of use was caused by a clinical trial for the purpose of receiving an authorisation to launch a medicinal product in accordance with the law on pharmaceutical products if an application concerning such a clinical trial was filed long after the registration of the trademark or there was insufficient funding to complete the trial.

7. Registration of a Letter Combination / Acronym as a Trademark

Not every combination of letters is an acronym, but every acronym is a word. The decision whether a particular letter combination is an acronym

depends on its perception by the native speaker, and in case of trademark registration, by the target group of consumers of the respective goods.

A letter combination perceived as an acronym by the target consumer group is a word, therefore it does not fall within the restrictions of Article 1483.1 of the CC RF.

A letter combination, which is not perceived as an acronym by the target consumer group, is not a word, therefore it does fall within the restrictions of Article 1483.1 of the CC RF and may not be registered as a trademark.

Ruling of the IPC Presidium dated 10 December 2021 in case No. SIP-255/2021

Gazprom Neft company filed an application to Rospatent for registration of the sign ГПН as a trademark. Rospatent registered the sign claimed in application as a trademark indicating the letters 'ГПН' (GPN) as a non-protectable element because it failed to meet the requirements of Article 1483.1 of the CC RF. The trademark owner contested this decision by Rospatent arguing the element in question was a word and had a distinctive character, so legal protection must be provided to the word alongside with the visual element. Rospatent dismissed the objection.Then, the trademark owner filed an appeal to the IPC against Rospatent's decision. The first instance court granted the appeal on the following grounds.The first instance court ruled that Rospatent's conclusion that the letter combination "GPN" in the contested sign had no distinctive character because it was not a word, was unfounded because, from the point of view of the Russian language, an acronym is a word made by abbreviating one, two or more words.

As the first instance court stated, in order to recognize a particular letter combination as an acronym, it must be proven that this letter combination is perceived by consumers of a particular goods as a word with a particular meaning, i.e., not every letter combination is an acronym but every acronym is a word. The assessment of whether a particular letter combination is an acronym depends, however, on its perception by the native speakers of the language and, in the case of registration of a trademark, by the target group of consumers of the goods concerned.

The first instance court stated that the GPN sign was a Russian-language acronym made by putting together three letters from the words GazProm Neft used by the applicant in the arbitrary part of the company name. The remedial measure applied by the first instance court was to order Rospatent to grant full legal protection to the sign claimed in the application. The IPC Presidium upheld the the first court's decision for the following reasons.

Pursuant to Article 1483.1 of the CC RF, signs that lack distinctive character shall not be granted state registration as trademarks.

According to Para 4, Clause 34 of the Rules for the Preparation and Submission of Documents as Basis for Legal Actions for State Registration of Trademarks and Service Marks approved by Order No. 482 of the Ministry of Economic Development of the Russian Federation dated 20 July 2015, signs lacking distinctive character include individual letters and letter combinations that do not have a verbal character or are not perceived as words.

An acronym is a word from the point of view of the Russian language. For a particular letter combination to be recognised as an acronym, it should be demonstrated that consumers of a particular goods perceive the letter combination as a word with a particular meaning. Not every letter combination is an acronym, but every acronym is a word. At the same time, the judgment as to whether a particular letter combination is an acronym depends on the perception of the letter combination by native speakers and, in the case of trademark registration, by the target group of consumers of the goods concerned. Thus, a letter combination perceived as an acronym by the target group of consumers is a word and therefore does not fall under the restrictions of Article 1483.1 of the CC RFA letter combination that is not perceived as an acronym by the target group of consumers is not a word and therefore does fall under the restrictions of Article 1483.1 of the CC RF. However, the Presidium acknowledged that, while correctly interpreting the applicable rules of law, the first instance court had nevertheless failed to establish the facts of the case in accordance with its own interpretation (whether the letters 'GPN' are perceived as an acronym). The case was therefore referred back to the first instance court for a new hearing.

8. Party's Interest in Trademark Invalidity Proceedings Under CC RF Article 1512.2.6

A person's interest in filing a challenge under Article 1512.2.6 of the CC RF is established depending on which procedure, administrative or judicial, was used to establish the trademark's rightholder unfair behaviour.

Where unfair behaviour is established using the administrative procedure, interest shall be found subject to the requirements of the anti-monopoly legislation, including its concept of an interested person — one whose rights and legitimate interests are affected by the anti-monopoly proceedings. Such persons will include those who were involved in the anti-monopoly proceedings (the applicant and those brought into the proceedings as interested persons) and their legal successors.

Where unfair behaviour is judicially established , such interest will follow from Article 4 of the Code of Commercial Procedure of the Russian Federation (CCP RF): interest in filing the challenge will be established on the basis of the scope of that specific person's recognised right of claim in the proceedings leading to possible declaration of certain actions as unfair competition, and on which persons have been brought into the judicial proceedings as third parties on the claimant's side.

Ruling of the IPC Presidium dated 10 December 2021 in Case No. SIP-481/2021

The Akademkniga Publishing House brought a challenge before Rospatent, invoking CC RF Article 1512.2.6 and referring to the fact that an IPC judgement in Case No. SIP-389/2019 found actions taken by the Nauka Publishing House to acquire and use the Akademkniga trademark to be an act of unfair competition.

Rospatent dismissed the challenge as it found the Akademkniga' lack of interest to in challenging the registration of the contested trademark in respect of the goods and services listed in its certificate. Rospatent proceeded from the fact that the Akademkniga Publishing House was legitimately interested in challenging the protection in respect of goods and services related to publishing business only, while for other goods and services the said entity's interest could not be established, for those either did not result from book publishing activities, are not related to printed or typographic matters, or to any publishing houses' services. On the other hand, Rospatent had already deleted the goods related to publishing business from the contested trademark's registration list. The Akademkniga disagreed with that decision and initiated proceedings at the IPC.

The first instance court overruled the Rospatent decision as it held that, according to CC RF Article 1512.2.6 and CCP RF Article 16, Rospatent was not entitled to re-assess the facts established in Case No. SIP-389/2019, and particularly to interpret the contents of the IPC decision in establishing the Akademkniga Publishing House's interest.

The IPC Presidium upheld the first instance judgment and noted the following. According to CC RF Article 1512.2.6, the registration of a trademark may be challenged and fully or partially invalidated anytime during the validity of the legal protection if its proprietor's actions related to the registration of that trademark in question or another trademark that is similar to the degree of confusion, have been duly found abusive or an act of unfair competition. According to CC RF Article 1513.1, the registration

of a trademark may be challenged on the grounds and within time frames provided for by CC RF Article 1512, by filing a challenge with the intellectual property office (Rospatent). According to CC RF Article 1513.2, invalidity proceedings on the ground provided for by Article 1512.2.6 of that Code may be initiated by an interested person.

As clarified in Para 169 of the Resolution No. 10, according to Article 14.4.2 of the Law on the Protection of Competition, subject to CC RF Article 1513.2, an interested person (i.e. one whose rights have been infringed by an act of unfair competition) may challenge the registration of a trademark where the rightholder's actions related to the registration of that trademark, or another trademark that is similar to the degree of confusion, have been found to constitute unfair competition (NB where actions involving the use of the trademark only, but not the acquisition thereof, are found to constitute unfair competition, that will not be a ground for challenging the trademark registration). After receiving a submission with the judgment or the anti-monopoly authority's decision attached, Rospatent will invalidate the legal protection granted to the trademark (CC RF Article 1512.2.6).

The IPC Presidium noted that the interest of the person who challenges the registration on the ground provided for by CC RF Article 1512.2.6 must be established depending on which procedure, administrative or judicial, has been used to establish unfair behaviour in the specific case. Where unfair behaviour is established using the administrative procedure, interest shall be found subject to the requirements of the anti-monopoly legislation, including its concept of an interested person — one whose rights and legitimate interests are affected by the anti-monopoly proceedings. Such persons will include those who were involved in the anti-monopoly proceedings (the applicant and those brought into the proceedings as interested persons) and their legal successors.

Where unfair behaviour is judicially established (Para. 61 of Resolution No.2 of the Plenum of the Supreme Court of the Russian Federation 'On Some Issues Arising from the Application of the Anti-Monopoly Legislation by Courts' dated 4 March 2021[1]), such interest will follow from CCP RF Article 4: interest in filing the challenge will be established on the basis of the scope of that specific person's recognised right of claim in the proceedings leading to possible declaration of certain actions as unfair competition, and on what persons have been brought into the judicial proceedings as third parties on the claimant's side.

[1] SPS Consultant Plus.

In respect of those persons, the fact of the specific person's interest and the scope of their legal claims have already been established by the anti-monopoly authority or court, and it is in that specific scope that the person is interested in filing the challenge. In view of the foregoing, the IPC Presidium held that Rospatent should have taken into account the outcome of the proceedings concerning the violation of anti-monopoly legislation: whether the acquisition of the exclusive right to the contested trademark / service mark had been found an act of unfair competition in full or in part.

It cannot be inferred from the IPC judgement in Case No. SIP-389/2019 that actions by the Nauka Publishing House related to the acquisition and use of the exclusive right to the trademark were found to be an act of unfair competition in respect of any concrete goods or services from that trademark's certificate. On the contrary, in its judgement the IPC found the Nauka acted in bad faith in respect of all the goods and services covered by that the contested trademark.

The very fact that the court found the acquisition of the exclusive right to the trademark in its entirety to be an act in bad faith indicates that the court proceeded from the applicant's right of claim in that scope. In view of this, the office should have granted the application in full and found the registration of the trademark invalid, because the IPC judgement in Case No. SIP-389/2019 stated that the acquisition by the Nauka Publishing House of the exclusive rights to the contested trademark without any disclaimers was an act of unfair competition.

9. A Trademark U ed in Altered Form

The use of a sign in a different language alters the trade mark's essence and cannot confirm the fact of trademark use for the purposes of the application of CC RF Article 1486 (trademark revocation for non-use).

Ruling of the IPC Presidium dated 6 December 2021 in Case No. SIP-880/2020

An applicant filed a claim for early termination of legal protection for the MAXIMUS, МАКСИМУС, MAXIMUS, and МАКСИМУС trademarks in respect of a number of goods items.

The first instance court granted the claim in part. The court found that the respondent was using trademarks containing the MAXIMUS verbal element but not the МАКСИМУС verbal element. The court also noted that in their documentation, the MAXIMUS sign spelt in Latin script was used

to identify the contested kinds of goods, while the above two trademarks' verbal elements were in the Cyrillic script, which testifies to an alteration of individual elements that transforms the essence of those trademarks.

The respondent appealed on points of law, arguing that the trademarks containing the MAXIMUS and МАКСИМУС verbal elements, whether in Cyrillic or Latin script, were perceived by the consumer in the same way and, consequently, the grounds cited to confirm the use of trademarks with the MAXIMUS verbal elements also confirmed the use of those including the МАКСИМУС verbal element.

The IPC Presidium disagreed with that argument and noted the following.

CC RF Article 1486.2 allows minor deviations between the form in which a trademark is registered and the form in which It is used, and deviations from the form in which it was originally registered. A mandatory condition for continued protection of a trademark is that it may only be used with such differences that do not alter the trademark's characteristic features. Based on the above provision, the IPC Presidium concluded that the use of a trademark in a significantly altered form (alphabet, verbal element appearance, and added or modified figurative and non-protectable elements), i.e., in a form that alters its distinctive character, does not constitute the use of such trademark in the sense of CC RF Article 1486.

According to Article 5.C.2 of the Paris Convention, the use of a trademark by its proprietor in a form differing in elements which do not alter the distinctive character of the sign in the form in which it was registered in one of the Union countries shall not entail invalidation of the registration and shall not diminish the protection granted to the mark.

That provision permits the existence of minor deviations between the form in which a mark is registered and the form in which it is being used, and deviations from the form in which it was first registered.

Nevertheless, the use of a sign in a different language alters the essence of the trademark. A similar position is reflected in the ruling of the IPC Presidium dated 21 May 2018 in Case No. SIP-335/2017.

10. Methodology for Establishing a Combined Sign's Similarity

The importance of a figurative element in a combined sign depends on how unique the element is, what role it plays in the layout of the image claimed in the application and how coherent it is with the sign's overall composition.

It should also be taken into account to what extent the verbal equivalent of the trademark's figurative element is correlated with its verbal element (e.g., whether the figurative element is a visual representation of the verbal element).

Ruling of the IPC Presidium dated 3 December 2021 in Case No. SIP-1086/2020.

Rospatent received an application for the registration of the 'РЛС' sign as a trademark. The office refused to register the sign as it did not conform to CC RF Article 1483.3.1, because the 'РЛС' ('RLS') element reproduced a sign used by the RLS-Patent company for the same kind of goods and services; furthermore, it did not conform to CC RF Article 1483.6.2, because there was a risk of confusing the sign with the trademarks («РЛС АПТЕКАРЬ», «РЛС ДОКТОР», «РЛС», «RLSNET») registered for that company. An appeal against that decision was also dismissed.

The IPC set aside the Rospatent decision as regards the sign's non-conformity to CC RF Article 1483.3.1 because Rospatent had not complied with the established methodology for assessing a sign's conformity to the said rule.

As regards the sign's non-conformity to CC RF Article 1483.6, the IPC upheld the Rospatent decision for the following reasons.

After analysing the contested sign and the opposed trademarks, the first instance court established that these included the 'РЛС'/'RLS' alphabetic element. It was a strong element that connected the confronted trademarks into a series.

The first instance court upheld Rospatent's conclusion that it were the above elements that had to be compared in assessing the similarity between the combined word sign claimed and those opposed to it by graphic and phonetic criteria. The contested sign's specific graphic execution does not preclude reading its 'РЛС' graphic element nor does it lead to a qualitatively different perception. Given the similarity between the compared signs' strong elements that makes them nearly identical, the court found a high degree of similarity between the contested sign and the opposed trademarks. In so doing, the court took into account that the RLS-Patent company had a series of trademarks sharing a common strong element with the contested sign.

In line with the explanations given in Para 162 of Resolution No. 10, in comparing combined signs, their strong and weak elements should be identified first of all. Further analysis will depend on which elements of the signs compared are similar/identical: strong or weak ones.

In examining the significance of an element in a combined sign, one should take into account its visual domination that may result both from the element's larger dimensions and from its more visible location in the layout (e.g., the element may occupy the central place from which image viewing begins).

An element's significance in a combined sign also depends on how much the element supports the performance of the sign's basic function. i.e., its ability to distinguish certain manufacturers'/providers' goods and services from others'. In a combined sign comprising a figurative element and a verbal one, the verbal element is usually the principal one, for it is easier to remember than the figurative one, so the consumer's perception focuses on it. The importance of the figurative element in a combined sign depends on how unique the element is, what role it plays in the layout of the subject sign and how coherent it is with the sign's overall composition. It should also be taken into account to what extent the verbal equivalent of the trademark's figurative element is correlated with its verbal element (e.g., whether the figurative element is a visual representation of the verbal element).

11. Assessing a Sign's Similarity to an Appellation of Origin

A combined sign cannot be found to resemble an appellation of origin exclusively on the basis of similarity between the verbal elements which establish the goods' relation to a certain geographical site.

Ruling of the IPC Presidium dated 3 December 2021 in Case No. SIP-144/2021

The Contested Sign

Rospatent refused to register the sign at issue for a broad range of ICGS Class 29 and 30 goods and services on the grounds that it failed to meet the provisions of CC RF Articles 1483.6.2 and 1483.7, as the sign was similar to the degree of confusion to earlier trademarks and similar to protected appellations of origin. The applicant's administrative appeal was dismissed, so it initiated appeal proceedings at the IPC. The court's first instance judgement granted the applicant's claims and declared Rospatent's decision invalid as it failed to meet the requirements set in CC RF Article 1483.7 and 1483.6.2. The administrative agency that was obligated to re-consider the

applicant's challenge appealed to the IPC Presidium, but its claims were dismissed and the first instance judgement upheld.

As regards the sign's conformity to CC RF Article 1483.6.2, the IPC Presidium upheld the first instance court's finding that Rospatent had made its conclusion by comparing a weak element of the contested sign ('Siberia') with other signs ('SIBERIA' / 'SIBEERIA' / 'SIBERRYA' / 'SIBERIYA'), without analysing other elements of the contested sign. In so doing, Rospatent departed from the similarity assessment methodology contained in Para. 162 of Resolution No. 10. The first instance court also rightfully noted that Rospatent did not err in refusing to exclude the weak verbal element from the contested sign. The IPC Presidium further upheld the first instance court's conclusion that Rospatent had not followed the methodology for assessing the contested sign versus the appellations of origin opposed to it. Proceeding from the provisions of CC RF Article 1483.7, from the Rules No. 482 and from the explanations in Para. 162 of Resolution No. 10, the IPC Presidium pointed to the following.

The contested sign containing the terms 'Магия Алтая' (Magic of the Altai) was confronted to the earlier appellations of origin No. 142 'Алтайский мед' (Altai Honey) and No. 193 'Мед горного Алтая (Honey of Mountain Altai). After highlighting the 'Altai' / 'of Altai' verbal elements and focusing on them, Rospatent found the signs compared to be similar. As the first instance court noted, in so doing Rospatent failed to establish the degree of similarity between the contested sign as it was applied for and the opposed appellations of origin, a prerequisite for establishing likelihood of confusion.

The IPC Presidium held that the parties to the proceedings did not dispute the obvious fact that the compared signs included the 'Altai' / 'of Altai' verbal elements. Rospatent found that elements to be strong in each of the signs at issue and continued comparing them with that in mind. However that office's conclusion contradicts its own statement that the element at issue only points at the goods' link to a specific geographic site, namely Altai.

Rospatent's position in respect of the strength of the sole element pointing at a geographical site (the Altai) and the justification of the similarity of the signs at issue by reference to the use in common of that element only essentially render the name of the geographical site and its derivative words 'monopolised' by the persons who were the first to obtain the exclusive right to a distinctive sign containing such an element.

After finding the 'Altai' / 'of Altai' ('Алтая'/ 'Алтайский') verbal elements to be strong in each of the signs in question, Rospatent continued

comparing the signs on that basis. Thus, in analysing graphical, phonetic, and semantic similarity between the sign claimed in the application and the opposed appellations of origin, the office was proceeding from an erroneous conclusion about the strong and weak elements in the signs compared.

II. Patents

1. Establishing Priority on the Basis of a Divisional Application

The CC RF allows the filing of a divisional application for a utility model separated from an application for an invention , and vice versa, provided that the original application discloses the technical solution that the divisional application seeks to protect.

Ruling of the IPC Presidium dated 13 December 2021 in case No. SIP-482/2021

The IPC considered a request to declare invalid and unenforceable Para. 20.12.2.4 of the Administrative Rules on reviewing, examining and granting utility model patents by Rospatent as approved by Ministry of Science and Education of the Russian Federation Order No. 326 dated 29 October 2008 ("the Administrative Rules") with regard to the possibility of establishing the priority of a divisional utility model application based on the original application for an invention. According to the applicant, the contested paragraph is wrong because the law does not explicitly provide for the very possibility of dividing a utility model application from an original invention application.

Dismissing the claim, the first instance court stated that Para 20.12.2.4 of the Administrative Rules conformed with the provisions of CC RF Articles 8, 128, 1226, 1357, 1379, 1384.4 and Article 4G of the Paris Convention for the Protection of Industrial Property of 20 March, 1883.

The IPC Presidium upheld the findings of the lower court and dismissed the cassation appeal. It explained that the contested paragraph of the Administrative Rules allowed the determination of the priority date, which was recorded by Rospatent when conducting its administrative operations, whereas the establishment of the priority of the divisional application was not in itself subject to the competence of the administrative body. The contested provision of the Administrative Rules is based on the civil law rule contained in CC RF Article 1381.4, which it implements. The purpose of this norm is to define the content of the subjective civil rights of the rights-

holders, to specify their absolute civil relations with all third parties, and not the exercise of the administrative body's authority (office's right to set or not to set a specific priority date by its decision).

In view of this and proceeding from the hierarchy of norms, the IPC Presidium agreed with the first instance court that it was required to check whether the contested paragraph of the Administrative Rules conformed with the civil law provision in CC RF Article 1381.4, and the meaning of this provision had to be determined by establishing whether or not it prohibited the division of the utility model application from the original invention application. The Court held that CC RF Article 1381.4 provided that, if all conditions were met, the priority of an invention, utility model or industrial design in a divisional application should be determined by the filing date of the original application or, if applicable, an earlier priority date. This provision does not introduce restrictions in the sense that the original application and the divisional application must relate to the same subject matter of the patent right. The relations between the applications are expressed as follows: the invention, utility model or industrial design in the divisional application must be disclosed in the original application. The IPC Presidium agreed with the interpretation by the first instance court that this relation should be interpreted as the requirement to disclose technical solutions, irrespective of the legal qualification. Both the utility model and the invention are technical solutions, and the scope of legal protection for technical solution claimed in the application (including that defined by the relevant utility model or invention patent) is determined by the applicant's will. Thus, the provisions of CC RF Article 1381.4 allow the separation of a divisional utility model application from an invention application and subsequentfiling, and vice versa.

Following the above interpretation, the IPC Presidium agreed with the conclusions of the first instance court that the provisions of CC RF Article 1381.4 imply the following: a divisional application must be related to the technical solution that is contained in the original application; at the same time, the qualification of the technical solution in the original application and in the divisional application (invention or utility model) does not need to be the same, nor does the divisional application need to request the same title of protection (patent for invention or utility model patent) that the original application does. The IPC Presidium further has clarified that the CC RF rules on the priority of an invention, utility model, industrial design under a divisional application are focused on protecting the rights of the applicant (the person entitled to file a patent), on granting the applicant

legal protection for their intellectual property. This legal instrument aims at protecting the rights of the patent holder to the technical solution disclosed in the original application.

Information about the authors:

N.I. Kapyrina — PhD, Assistant Professor.

M.A. Kolzdorf — LL.M., Lecturer.

Contribution of the authors:

N.I. Kapyrina — part 1– 4, 6, 11, II.

M.A. Kolzdorf — part 5,7– 9, 10.

The article was submitted to the editorial office 22.04.2021; approved after reviewing 05.05.2022; accepted for publication 11.05.2022.

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

Book Review

Review
DOI:10.17323/2713-2749.2022.2.141.147

An Innovative Fundamental Doctrinal Course in Theory of State and Law

Vladimir Mihailovich Baranov

Nizhny Novgorod Academy of the Interior Ministry, 3 Ankudinovskoye Shosse, Nizhny Novgorod 603950, Russia, baranov_prof@bk.ru, orcid.org/0000-0003-2689-739X

Abstract

Review of the book: Theory of State and Law. V. B. Isakov (ed.) et al. Moscow: Norma, 2020. 1864 p. Vol. 1: Theory of State and Law: Curriculum. 176 p. Vol. 2: Theory of State and Law: Textbook for Schools of Law. 656 p. Vol. 3: Theory of State and Law: Tutorial. 488 p. Vol. 4: Theory of State and Law: Game Tutorial. 544 p.

Keywords

theory of state and law, doctrine, innovative course, practicum, legal categories, legal rducation

For citation: Baranov V.M. (2022) An Innovative Fundamental Doctrinal Course in Theory of State and Law. *Legal Issues in the Digital Era*, vol. 3, no 2, pp. 141–147. DOI:10.17323/2713-2749.2022.2.141.147

In the current Russian book market, there is no dearth of editions on theory of state and law, with textbooks and learning materials on the subject occupying long shelves at bookshops. Most of these were written by prominent authors and established research institutions and are re-issued annually. A really innovative publication can seldom be seen on the shelves. For this

reason, among others, the training course in the theory of state and law in four books, developed by the researchers of the Theory and History of Law Chair, of Law Department, the Higher School of Economics (National Research University), will certainly attract the interested reader's attention.

The series of learning aids opens with a curriculum for the course in the theory of state and law, published in a separate volume. Notably, training course curricula have evolved for the worse in the recent years as they turned from a plan, intended simply to guide students through the subject, into a cumbersome and bureaucratic reporting document for various regulatory authorities. The author of the curriculum under review has generally managed to avoid this problem. Its content is free from bureaucratic frills and focuses directly on the tuition process. It includes a thematic plan of the discipline to be taught, discussion class outlines, definitions of the main concepts, reference lists, self-evaluation quizzes; topics for essays, abstracts, term and graduation papers; knowledge and skill evaluation criteria; and examination and credit quiz questions.

However, we should ask whether that technical document really had to be printed as a separate edition for the general reader; but the publication seems quite reasonable. The curriculum represents a 'control hub' for the entire set of learning aids and contains its 'genome'. All the other volumes are co-ordinated in some way or other on the basis of the curriculum. Besides, both students and teachers will probably be pleased to look into the curriculum, published as a handsomely designed book, at a training session or examination.

The second volume in the series is also traditionally named and designed as a Textbook. Amid today's information redundancy, with a wealth of information on any subject available to students in real time, textbooks have largely lost their former significance. From 'kings' of the tuition process they have turned into ordinary 'cans' of information for learners, displaced by such readily available sources as online learning aids, articles in online journals, database analytics, online courses, etc. Yet the textbook is far from becoming useless as a practical tuition tool. It remains in demand as an acknowledged review of the subject for students who read for their examinations and need a systematic account in the optimal volume to be internalised. In this respect, the Textbook under scrutiny meets all reasonable requirements: a volume that students can digest (656 pages), well-structured content, and a clear 'textbook' style.

The general concept behind the Textbook is formulated in one of its first topics: "The authors of this textbook proceed from the fact that law is a multi-faceted social phenomenon showing its various facets in vari-

ous areas of jurisprudence. So its topical chapters such as 'Rules of Law', 'Legal Relations', and 'Application and Interpretation' are mainly based on a normative approach to law. That is the key approach to legal education because the application and interpretation of legal rules have always been the legal practitioner's main tasks. However, already in the chapter entitled 'Rule Making, and Norm Creation Process' we have to accept a broader approach, for a legal rule and especially a normative legal act cannot be developed on the basis of knowledge about law itself: we also need to know the object of legal regulation and the legal relations to be codified. The 'Human Rights', 'Rule of Law', and 'Legality, Legal Order, and Discipline' topics are based on a sociological approach to law that is pivotal to understanding as well as critical evaluation of rules of law. In the topic entitled, 'Legal Consciousness and Legal Culture', law is understood as a socio-cultural phenomenon and a manifestation of human consciousness. In short, even after leafing briefly through the textbook one can find that it offers a broad spectrum of approaches to such a complex and multi-faceted phenomenon as law is' (pp. 51–52). To put it differently, the Textbook' authors spared both themselves and their students the trouble of pursuing just one of the existing approaches to law in the entire edition, and proceeded pragmatically from a multi-aspect and integrative approach to legal understanding.

We shall avoid the temptation of examining the Textbook's topical chapters and arguing with the authors on specific issues. Of course, the Textbook cannot encompass the entire spectrum of state and legal theory approaches and views on various issues — or claim to do so. Most importantly, on its pages we found no opinions that could be considered backward, erroneous, inferior, or misleading to students. As for the controversial points that are present, these can be discussed on more detailed examination.

Let us dwell upon some other features that distinguish the Textbook under scrutiny from other similar publications.

Its table of contents already points to an 'unbalanced' coverage of state and law issues, with much more space given to law than to state-related issues. One of the authors explained to us that, according to an agreement between the HSE Law Department's chairs, the matters concerning the state and political system are considered in more detail in the course in constitutional law that runs parallel to the course in the theory of state and law under the general curriculum. However, in the examination cards, state-related issues are present in their entirety, as covered in both courses — those of theory and constitutional law. It is therefore a good idea for teachers to keep this feature in mind as they use this book.

An advantage of the Textbook under review as compared to other publications is that it contains a lot of diagrams on the theory of state and law — about one hundred, i.e. a sizable album of diagrams related to the course is integrated into it. These include more or less successful ones, which also requires a separate review.

The reader will certainly pay attention to the authors' attempt to visualise the 'concept list' related to each topic. Much has been said about the concept lists and their significance for research and educational practice, but, to the best of our knowledge, this is the first attempt to present concept lists in diagram form. Of course, some of the diagrams are not perfect: in our opinion, some concept lists are incomplete or contain alien categories. Yet the approach itself, namely the tentative schematic representation of concept lists, can only be welcomed. A clear understanding of the content of legal categories' concept lists is useful for addressing a multitude of tasks — identifying inter-disciplinary relationships, retrieving information, translating scholar terms correctly into foreign languages, etc.

We should note some other interesting features of this edition. Each topic opens with a 'minor introduction', a literary scene or interesting introductory information of a general social nature. Senior students might find such exemplification redundant, but, given that the theory of state and law is taught in the first year of reaching, it is helpful to first-year students as it graphically relates theory to life and practice and invites a deeper proactive understanding of the theory.

Each topical chapter includes a self-evaluation quiz, and the Textbook itself is supplemented with a list of examination questions. Those follow naturally from the course's curriculum and are also repeated in the Tutorial. However we believe the repetitions to be justified in this case, for Russian universities may not be rich enough to buy all the three inter-related publications, namely the curriculum, textbook and tutorial, for each student. So each book in the series is a complete source in its own right that can be used either as part of the system or individually.

We now open the next volume in the learning aid series, the Tutorial. A university lecturer has probably had an opportunity to see or even develop methodological guides of similar purpose. These are usually smaller learning aids produced reprographically for the students. In this perspective, the inclusion of a tutorial as a separate printed book in this series seems a risky affair. Will such a publication be flexible enough to meet the fast-changing needs of the tuition process? Or will it become outdated even before it reaches the student?

The Tutorial's table of contents shows the volume pursues three goals: firstly, it aims to help the students prepare for discussion sessions; secondly, to assist them in organising their homework; and, thirdly, to give advice and guidance to online learners of the course in the theory of state and law.

The Tutorial starts with a review of university-level learning modalities and methods for organisation and self-organisation in the learning process, which is relevant to first-year students. This is followed by plans of sessions on all the twenty-four topics of the course that include basic terminology, a tentative plan of the seminar, a home task, problems and case studies, topics for essays and reports, etc.

Among the entire traditional set of methodological guidance, only the home task — rigidly defined for each topic — may seem questionable because it is usually a formalised one: to develop a diagram, fill in a table, etc. What can a lecturer do in this situation if s/he wants to be creative and go beyond the tutorial? The answer is contained in the final book, the Game Tutorial, that contains alternative home task options and encourages creative teaching.

In addition to session plans, the Tutorial includes many other useful things for students: topics for term and graduation papers (in both Russian and English), recommendations for writing them, a list of examination and credit quiz questions and recommendations on reading for them, and a list of problems and case studies. As noted above, recommendations on each topic are given to online learners of the theory of state and law.

The tentative outlines of answers to examination cards (pp. 327-486) are probably the most singular part of the tutorial. Though entitled 'Plans of Answers', on close examination these turn out to be synopses — concise answers to the examination questions, rather than outlines. Students will certainly appreciate this approach, for it is actually a ready-to-use product that students should simply memorise and then dilute with some freshet at the exam.

That said, this methodological innovation suggested by the authors raises questions. Firstly, the most inert and spiritless students will never read the textbook itself and confine themselves instead to the tentative plans of answers, for the latter are easier to read and contain the same information in a quarter of the full volume! True, their final mark will be 'C', but that will be quite enough for some. Secondly, the plans of answers developed by professors make perfect raw stuff for cribs approved at the 'top level'. Imagine anybody saying there's something wrong about them! Thirdly, printed

outlines of answers are psychologically perceived as a standard and may lead some students to challenge their examination marks: 'I give the standard answer and you give me a 'C'!" The teaching practice will soon show whether our apprehension is well-founded.

And, finally, the fourth and most innovative part of this series of learning aids is the Game Tutorial intended for lecturers of the theory. For fairness' sake, it is the chair's second attempt to publish a learning aid for teachers rather than students. The first one was a learning aid entitled 'Game Tutorial: Some Experience of Teaching Fundamentals of Law at the Higher School of Economics' and published in 2015. Some ideas and approaches from that tutorial have migrated into its current, far more advanced version. What does this learning aid contain and how can it help lecturers?

The Game Tutorial opens with a detailed review of the forms and methods of teaching the theory of state and law. The ordinary Tutorial contains a similar review as well, but here it is more elaborate and has a different focus. For virtually all the modalities, it shows not only their current status but also their development prospects in the existing conditions.

The Game Tutorial's biggest section contains methodological guidance for each of the twenty-four topics of the course. It describes the purposes of teaching the topic, home task options, problems, case studies, business games, and workshops, and also contains a tentative list of evaluation questions and a recommended reading list for the lecturer. The tasks, problems, case studies, business games and especially the topical issues may be used not only in class but also in extracurricular work with students such as academic competitions and question-and-answer sessions.

The Game Tutorial includes a collection of problems and case studies, also a broader one than that offered to the students in the Tutorial.

Lecturers will certainly pay attention to a collection of games and workshops — active tuition modalities that can be used in the course of the theory of state and law. Comments to these show the practice of using them at the Law Department of the Higher School of Economics.

The Game Tutorial concludes with a section under the title 'Problems, Plans, Prospects' where the authors share their views on ways of overcoming the crisis of traditional learning modalities at higher school. Experimental curricula in the theory of state and law are suggested, with a reduced number of lectures or with all of them replaced with active learning exercises.

According to the introductory article to the whole edition, included in the course's curriculum, the authors' general intention was to write a series of publications catering to all the needs of the tuition process rather than an individual textbook. They have certainly done a lot towards this goal and produced an innovative kit of learning aids comprising four volumes. It contains both controversial aspects points and some undeniable achievements. In the next few years, university practice will show how successful it will be.

A fleet of four volumes is now departing from the bookshop counters, and we shall watch with sympathetic interest how its voyage will develop.

Information about the author:

V.M. Baranov — Professor, Doctor of Sciences (Law), Assistant Director for Innovative Development of Research Activities, Merited Lawyer of the Russian Federation.

The review was submitted to the editorial office 30.04.2022; approved after reviewing 12.05.2022; accepted for publication 20.05.2022.

Legal Issues in the **DIGITAL AGE**

AUTHORS GUIDELINES

The submitted articles should be original, not published before in other printed editions. The articles should be topical, contain novelty, have conclusions on research and follow the guidelines given below. If an article has an inappropriate layout, it is returned to the article for fine-tuning. Articles are submitted Word-processed to the address: lawjournal@hse.ru

Article Length
Articles should be between 60,000 and 80,000 characters. The size of reviews and the reviews of foreign legislation should not exceed 20,000 characters.

The text should be in Times New Roman 14 pt, 11 pt for footnotes, 1.5 spaced; numbering of footnotes is consecutive.

Article Title
The title should be concise and informative.

Author Details
The details about the authors include:

- Full name of each author
- Complete name of the organization — affiliation of each author and the complete postal address
- Position, rank, academic degree of each author
- E-mail address of each author

Abstract
The abstract of the size from 150 to 200 words is to be consistent (follow the logic to describe the results of the research), reflect the key features of the article (subject matter, aim, methods and conclusions).

The information contained in the title should not be duplicated in the abstract. Historical references unless they represent the body of the paper as well as the description of the works published before and the facts of common knowledge are not included into the abstract.

Keywords
Please provide keywords from 6 to 10 units. The keywords or phrases are separated with semicolons.

References
The references are arranged as follows: [Smith J., 2015: 65]. See for details http://law-journal.hse.ru.

A reference list should be attached to the article.

Footnotes
The footnotes include legal and jurisprudencial acts and are to be given paginaly.

The articles are peer-reviewed. The authors may study the content of the reviews. If the review is negative, the author is provided with a motivated rejection.

Вопросы права **В ЦИФРОВУЮ ЭПОХУ**

ЕЖЕКВАРТАЛЬНЫЙ НАУЧНО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ

«Вопросы права в цифровую эпоху» — научный ежеквартальный электронный журнал, направленный на всесторонний анализ права в цифровую эпоху. Его главная цель заключается в рассмотрении вопросов, связанных с правовыми последствиями постоянно меняющихся информационных технологий.

Цифровая эпоха — это эпоха информационных и коммуникационных технологий, обусловливающих дальнейшее общественное развитие, в том числе с использованием цифровых данных. Но вместе с тем цифровое развитие выявляет пробелы в праве и потребность в новых правовых решениях.

“Вопросы права в цифровую эпоху” — журнал, который предоставляет возможность юристам — ученым и практикам — обмениваться мнениями. В том числе журнал поощряет междисциплинарные дискуссии по темам, находящимся на стыке права, технологий, экономики и политики в современном мире.

“Вопросы права в цифровую эпоху” — рецензируемый журнал. В нем применяется двойное “слепое” рецензирование присылаемых материалов.

Журнал приглашает авторов присылать статьи, отражающие результаты научных исследований регулирования цифровой среды. Редакция приветствует теоретические и компаративистские подходы, исследование перспектив правового развития в различных странах.

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и включен в реестр зарегистрированных средств массовой информации серия серия Эл № ФС77-83367

ISSN 2713-2749

Адрес редакции
Россия, 109028 Москва, Б. Трехсвятительский пер, 3,
офис 113
Тел.: +7 (495) 220-99-87
http://law-journal.hse.ru
e-mail: lawjournal@hse.ru

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Консультативный отдел

Учредитель
Национальный исследовательский университет «Высшая школа экономики»

Вопросы права
В ЦИФРОВУЮ ЭПОХУ

2/2022

ЕЖЕКВАРТАЛЬНЫЙ НАУЧНО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ ТОМ 3

Статьи

Комментарии

Рецензия

Научная статья

DOI:10.17323/2713-2749.2022.2.4.48

ИНТЕРНЕТ ВЕЩЕЙ: ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ

Богдан Юрьевич Дорофеев

Россия, Москва 109028, Большой Трехсвятительский пер., 3, офис 113, ved-intlaw@yandex.ru

Аннотация

Как известно, интернет стал важной частью социальной жизни, общественной и межличностной коммуникации, удобной формой и необходимым условием успешного функционирования экономики, средств массовой информации, гражданского общества. При этом, развиваясь технологически и функционально, интернет генерирует новые технические решения и новые возможности, приводящие к формированию новых концепций и терминов, в основе которых заложены технологические свойства интернета. Одним из таких новых решений является зарождение интернета вещей — комплексного технологического, технического и экономико-правового явления. В то время как комплексное понимание сущности интернета вещей в значительной степени еще формируется, уже отмечается ряд спорных моментов и вопросов, требующих в том числе и научно-правовых дискуссий. Настоящая статья посвящена вопросам понятия интернета вещей, анализу его объема и содержания, исследованию смысла и назначения термина «интернет вещей», его соотношению со смежными понятиями, и его роли в праве. Опираясь на изучение входящих в термин «интернет вещей» понятий «интернета» и «вещи», рассматривая интернет вещей как комплексную систему, автор исследует ее элементы, определяя их дефиниции, цели, раскрывая их роль в указанной системе. По результатам исследования автор приходит к выводу, что основным содержанием анализируемой системы является управление, осуществляемое с применением интернета (как информационно-технологической системы) и специальных технических средств. Исходя из указанного вывода, на основе анализа сущности интернета, термина интернета вещей и различных подходов, автор предлагает обобщенное определение интернета вещей как программно-технологической системы дистанционного управления удаленными объектами, осуществляемой в интересах пользователя с помощью интернета и технических свойств управляемых объектов, позволяющих проводить электронный обмен данными.

Ключевые слова

интернет, интернет вещей, промышленный интернет вещей, информация, информационно-технологическая система, управление вещами.

Для цитирования: Дорофеев Б.Ю. (2022) Интернет вещей: проблемы определения. *Вопросы права в цифровую эпоху*. Т. 3. № 2. С. 4–48 (на англ. яз.). DOI:10.17323/2713-2749.2022.2.4.48

Информация об авторе:
Б.Ю. Дорофеев — кандидат юридических наук, доцент.

Научная статья

DOI:10.17323/2713-2749.2022.2.49.72

ПРАВОВОЙ СТАТУС ЭМИТЕНТОВ КРИПТОАКТИВОВ С ТОЧКИ ЗРЕНИЯ ПРЕДЛАГАЕМОГО ПОСТАНОВЛЕНИЯ MICA

Яна Даудрих

Университет имени Я.А. Коменского, Словакия 81000, Братислава, ул. Шафариково наместье, 6, yana.daudrikh@flaw.uniba.sk, https://orcid.org/0000-0003-1297-5967/

Аннотация

В свете развития современных цифровых технологий встает вопрос о необходимости создания единого механизма регулирования эмитентов криптоактивов, включающего комплексное регулирование статуса всех субъектов, участвующих в торговле криптоактивами. Однако до сих пор мы отмечаем отсутствие единообразия и абстрактное регулирование основных субъектов, торгующих криптоактивами, вытекающее из V. AML директивы. Под давлением политиков и профессионального сообщества Европейская комиссия разработала проект долгожданного постановления MICA с целью обеспечения создания общего регулирования в области криптоактивов, которая будет применима во всех государствах-членах Европейского союза (далее — «ЕС»), включая государства-члены Единого экономического пространства (далее — «ЕЭП»). Предложенный Комиссией проект постановления MICA имеет целью унифицировать разрозненное правовое регулирование криптоактивов, которое государства-члены ЕС были вынуждены создать из-за отсутствия более масштабного регулирования этого института на уровне ЕС. Основной целью данной статьи является анализ вновь определенных институтов, включая категоризацию криптоактивов, охватываемых MICA. В этом контексте рассматриваются основные аспекты функционирования процесса эмиссии криптоактивов, включая обязанности публикации «white paper». Особо рассматривается роль Европейского банковского управления (European Banking Authority — далее «EBA») как надзорного органа над эмитентами известных криптоактивов. На основе анализа автор приходит к выводу, что применение положений MICA связано с рядом проблем, на которых затем останавливается более подробно. Неоднозначность в правовом применении MICA наблюдается, например, в случае регулирования понятий криптоактивов, которые носят общий характер, или в случае отсутствия более детального разъяснения сотрудничества между соответствующими органами ЕС и органами третьих стран, направленного на борьбу с отмыванием грязных денег и финансированием терроризма. При написании данной статьи были использованы следующие научные методы: формально-юридический, сравнительно-правовой, анализ, синтез, аналогия, индукция и дедукция.

Ключевые слова
MICA; криптоактив; отмывание грязных денег и финансирование терроризма; токен приложений; токен,привязанный к активам; токен электронных денег; white paper; надзор над эмитентами токенов.

Для цитирования: Даудрих Я. (2022) Правовой статус эмитентов криптоактивов с точки зрения предполагаемого постановления МИКА. *Вопросы права в цифровую эпоху*. Т.3. № 2. С. 49–71 (на англ. яз.). DOI:10.17323/2713-2749.2022.2.49.72

Информация об авторе:
Я. Даудрих — главный научный сотрудник, доктор права.

Научная статья

DOI:10.17323/2713-2749.2022.2.73.89

ЧАСТНАЯ ЖИЗНЬ РЕБЕНКА В ЦИФРОВОЙ СРЕДЕ: НОВЫЕ РИСКИ НЕ УЧТЕНЫ

Наталья Вячеславовна Кравчук

Институт научной информации по общественным наукам РАН, отдел правоведения, Москва, 117218, ул. Кржижановского, 15, стр. 2, natkravchuk@mail.ru

Аннотация
Цифровые технологии привели к появлению новых возможностей реализации и защиты прав человека. При этом многократно возросли и нарушения прав человека. Использование коммуникационных технологий влияет на каждодневную жизнь взрослых и тем более меняет жизнь детей. Риски, с которыми они сталкиваются за счет использования Интернета, усиливаются и усложняются. В контексте цифровых технологий по-новому проявило себя значение права ребенка на частную жизнь. Помимо безопасности, оно рассматривается в контексте обработки данных и «цифрового следа», оставляемого детьми. Родители, традиционно рассматривавшиеся в качестве лиц, играющих ключевую роль в руководстве детьми и их поддержке в реализации ими их прав в цифровом пространстве, в настоящее время стали основными поставщиками информации о своих детях в Интернет. При этом проблема «шэрентинга» (sharenting) остается не законодательно урегулированной как на национальном, так и на международном уровне. Меры, разрабатываемые для защиты права ребенка на частную жизнь, формируются на основе парадигмы оказания помощи родителям, а не их обязательства не придавать публичности информацию о ребенке. Замечание общего порядка № 25 о правах детей в связи с цифровой средой, принятое Комитетом ООН по правам ребенка в 2021 году, отражает этот подход. Позиция Комитета демонстрирует торжество восприятия ребенка как объекта неоспоримой власти и заботы родителя. Эта позиция препятствует рассмотрению онлайн-поведения родителей как потенциально вредного детям, а также разработке норм и средств защиты права ребенка на частную жизнь в ситуации его нарушения родителем.

Ключевые слова
права человека; права ребенка; право на частную жизнь; цифровая среда; родители; шэрентинг; Комитет ООН по правам ребенка.

Для цитирования: Кравчук Н. В. (2022) Частная жизнь ребенка в цифровой сфере: новые риски не учтены. *Вопросы права в цифровую эпоху*. Т. 3. № 2. С. 73–89 (на англ. яз.). DOI:10.17323/2713-2749.2022.2.73.89

Информация об авторе:
Н.В. Кравчук — старший научный сотрудник, кандидат юридических наук.

Научная статья

DOI:10.17323/2713-2749.2022.2.90.115

АВТОМАТИЗАЦИЯ СУДЕБНОЙ АТРИБУЦИОННОЙ ЭКСПЕРТИЗЫ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Татьяна Владимировна Романова

Факультет гуманитарных наук Национального исследовательского университета «Высшая школа экономики», профессор, 603155 Россия, Нижний Новгород, Большая Печёрская ул., 25/12, e-mail: tvromanova@hse.ru., ORCID: 0000-0002-1833-2711

Анна Юрьевна Хоменко

Факультет гуманитарных наук Национального исследовательского университета «Высшая школа экономики»; Центр экспертиз и исследований ЕСИН», 603155 Россия, Нижний Новгород, Большая Печёрская ул., 25/12, e-mail: akhomenko@hse.ru. ORCID: 0000-0003-3564-6293

Аннотация
В статье речь идет об апробации интегративного атрибуционного алгоритма. Он основан на анализе идиостиля автора письменного текста методами интерпретативной лингвистики с последующей объективацией полученных данных с помощью математической статистики. Алгоритм решает идентификационную проблему атрибуции. Выбор параметров, описывающих индивидуальный стиль автора, основан на рассмотрении текста как продукта аутентичной языковой личности. Языковая личность описывается с использованием психолингвистических (Ю.Н. Караулов), социолингвистических и судебно-лингвистических (С.М. Вул, M. Coulthard, W.Shuy) методов. Для проверки гипотезы, является ли интегративная методика наиболее эффективной при решении идентификационной задачи атрибуции, было создано электронное приложение «ХоРом», кумулирующее в себе описанные выше подходы к анализу языковой личности: http://khorom-attribution.ru/#/. С помощью ресурса можно сравнить две модели языковой личности и определить уровень их сходства посредством следующих метрик: коэффициента корреляции Пирсона, коэффициента детерминации линейной регрессии и t-критерия Стьюдента. Важно, что приложение также отображает интерпретируемую модель языковой личности, давая пользователю информацию о

значении показателей каждого параметра. Система имеет обширный функционал, включая выбор параметров, просмотр реализации параметров в тексте документа и внесение изменений в окончательный список реализаций параметров (при неточности программы пользователь имеет возможность исправить ее работу вручную). Созданное программное обеспечение является лишь частью атрибуционного алгоритма. Полученные данные математической статистики необходимо анализировать экспертным путем с помощью разработанных для алгоритма методических рекомендаций. Эффективность методики доказана посредством ее апробации на текстах разного объема и жанровой отнесенности: был проанализирован ряд текстов художественного, публицистического, официально-делового, обиходно-бытового стилей. Для текстов всех дискурсов, кроме обиходно-бытового, разработанный алгоритм показал высокий уровень точности (F-мера от 0,8 до 1). Для улучшения работы алгоритма на текстах обиходно-бытового стиля авторами исследования разработан ряд улучшений, планирующихся к внесению в алгоритм.

Ключевые слова
атрибуция, языковая личность, автоматическая обработка текста, лингвистическая модель, математическая модель, атрибутивное программное обеспечение, судебная автороведческая экспертиза.

Благодарности: Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-312-90022.

Для цитирования: Романова Т.В., Хоменко А.Ю. (2022) Автоматизация судебной атрибуционной экспертизы: проблемы и перспективы. *Вопросы права в цифровую эпоху*. Т. 3. № 2. С. 90–115 (на англ. яз.). DOI:10.17323/2713-2749.2022.2.90.115

Информация об авторах:
Т. В. Романова — профессор, доктор филологических наук.
А.Ю. Хоменко — кандидат филологических наук, эксперт.

КОММЕНТАРИИ

Обзор

DOI:10.17323/2713-2749.2022.2.116.140

ОБЗОР КЛЮЧЕВЫХ ПОЗИЦИЙ ПРЕЗИДИУМА СУДА ПО ИНТЕЛЛЕКТУАЛЬНЫМ ПРАВАМ

Наталья Игоревна Капырина

МГИМО (У) МИД России, Россия, Москва 119454, проспект Вернадского, 76, n.kapyrina@ my.mgimo.ru, ORCID: 0000-0003-1276-1600, Researcher ID: AAQ-3784-2021

Мария Александровна Кольздорф

Факультет права, Национальный исследовательский университет «Высшая школа экономики», Россия, Москва 101000, Мясницкая ул., 20, mkolzdorf@hse.ru, ORCID:0000-0003-3227-3348, Researcher ID: AAI-1625-2019

Аннотация

В обзоре освещены ключевые позиции из постановлений, принятых Президиумом Суда по интеллектуальным правам в декабре 2021 и январе 2022 гг. Президиум Суда по интеллектуальным правам рассматривает кассационные жалобы на решения суда первой инстанции, в частности, по делам, связанным с регистрацией объектов интеллектуальных прав и с оспариванием правовой охраны. В связи с этим обзор в основном посвящен вопросам охраноспособности объектов патентных прав и средств индивидуализации, а также отдельным процессуальным аспектам деятельности Роспатента и Суда по интеллектуальным правам. В текущем обзоре преимущественно рассмотрены различные вопросы, связанные с товарными знаками: противоречие общественным интересам; противопоставление более ранним товарным знакам или наименованиям места происхождения товара; обозначения, содержащие географические наименования; обозначения, вводящие в заблуждение; методика сравнения обозначений; досрочное прекращение правовой охраны в связи с неиспользованием товарного знака; недобросовестная конкуренция; различные процессуальные вопросы. В Обзоре также приведено постановление, в котором Президиум рассмотрел вопрос определения даты приоритета заявки о выдаче патента на полезную модель, выделенной из первоначальной заявки, поданной в отношении изобретения.

Ключевые слова

Российская Федерация, судебная практика, товарные знаки, прекращение охраны, сходство, недобросовестная конкуренция, общественные интересы, НМПТ, полезная модель, патент.

Для цитирования: Капырина Н.И., Кольздорф М.А. (2022) Обзор ключевых позиций Суда по интеллектуальным правам. *Вопросы права в цифровую эпоху.* Т. 3. № 2. С. 116–140 (на англ. яз.). DOI:10.17323/2713-2749.2022.2.4.48

Информация об авторах:

Н.И. Капырина — кандидат юридических наук, доцент.
М. А. Кольздорф— магистр, преподаватель.

Вклад авторов:

Н. И. Капырина — части 1,2,3, 4, 6, 11, II.
М.А. Кольздорф— части 5,7, 8, 9, 10.

Рецензия

DOI:10.17323/2713-2749.2022.2.141.147

ИННОВАЦИОННЫЙ ФУНДАМЕНТАЛЬНЫЙ ДОКТРИНАЛЬНЫЙ КУРС ТЕОРИИ ГОСУДАРСТВА И ПРАВА

Владимир Михайлович Баранов

Аннотация
Рецензия на книгу: Теория государства и права. Кн. 1– 4. М.: Норма, 2020. 1864 с. Кн. 1: Теория государства и права: программа курса / В. Б. Исаков. 176 с. Кн. 2: Теория государства и права: учебник для юридических вузов / Колл. авт. 656 с. Кн. 3: Теория государства и права: практикум / Колл. авт. 488 с. Кн. 4: Теория государства и права: игропрактикум / Колл. авт. 544 с.

Ключевые слова
теория государства и права; доктрина; инновационные курсы; категории права; юридическое образование.

Для цитирования: Баранов В. М. (2022) Инновационный фундаментальный доктринальный курс теории государства и права. *Вопросы права в цифровую эпоху*. Т. 3. № 2. С. 141–147 (на англ. яз.). DOI:10.17323/2713-2749.2022.2.4.48

Информация об авторе:
В.М. Баранов — профессор, помощник начальника по инновационному развитию научной деятельности, доктор юридических наук, заслуженный юрист Российской Федерации.

АВТОРАМ

Требования к оформлению текста статей

Представленные статьи должны быть оригинальными, не опубликованными ранее в других печатных изданиях. Статьи должны быть актуальными, обладать новизной, содержать выводы исследования, а также соответствовать указанным ниже правилам оформления. В случае ненадлежащего оформления статьи она направляется автору на доработку.

Статья представляется в электронном виде в формате Microsoft Word по адресу: lawjournal@hse.ru
Адрес редакции: 109028, Москва, Б. Трехсвятительский пер, 3, оф. 113
Рукописи не возвращаются.

Объем статьи
Объем статей до 1,5 усл. п.л., рецензий — до 0,5 усл. п.л.

При наборе текста необходимо использовать шрифт «Times New Roman». Размер шрифта для основного текста статей — 14, сносок — 11; нумерация сносок сплошная, постраничная. Текст печатается через 1,5 интервала.

Название статьи
Название статьи приводится на русском и английском языке. Заглавие должно быть кратким и информативным.

Сведения об авторах
Сведения об авторах приводятся на русском и английском языках:

- фамилия, имя, отчество всех авторов полностью
- полное название организации — места работы каждого автора в именительном падеже, ее полный почтовый адрес.
- должность, звание, ученая степень каждого автора
- адрес электронной почты для каждого автора

Аннотация
Аннотация предоставляется на русском и английском языках объемом 250–300 слов.
Аннотация к статье должна быть логичной (следовать логике описания результатов в статье), отражать основное содержание (предмет, цель, методологию, выводы исследования).

Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает…»).

Исторические справки, если они не составляют основное содержание документа, описание ранее опубликованных работ и общеизвестные положения, в аннотации не приводятся.

Ключевые слова
Ключевые слова приводятся на русском и английском языках. Необходимое количество ключевых слов (словосочетаний) — 6–10. Ключевые слова или словосочетания отделяются друг от друга точкой с запятой.

Сноски
Сноски постраничные.
Сноски оформляются согласно ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления», утвержденному Федеральным агентством по техническому регулированию и метрологии. Подробная информация на сайте http://law-journal.hse.ru.

Тематическая рубрика
Обязательно — код международной клас-сификации УДК.

Список литературы
В конце статьи приводится список литературы. Список следует оформлять по ГОСТ 7.0.5-2008.

Статьи рецензируются. Авторам предоставляется возможность ознакомиться с содержанием рецензий. При отрицательном отзыве рецензента автору предоставляется мотивированный отказ в опубликовании материала.

Плата с аспирантов за публикацию рукописей не взимается.

Выпускающий редактор *Р.С. Рааб*
Художник *А.М. Павлов*
Компьютерная верстка *Н.Е. Пузанова*