ГОСУДАРСТВО И ПРАВО, 2019, № 9, с. 117–130
STATE AND LAW, 2019, № 9, pp. 117–130

INFORMATION SECURITY IN IDENTIFICATION IN THE DIGITAL AGE: INFORMATION LAW ASPECT

© 2019 г. V. B. Naumov

Institute of State and Law of the Russian Academy of Sciences, Moscow

E-mail: nau@russianlaw.net

Received 06.09.2019

Abstract. This article deals with patterns in the development of legislation and the application of the law in identifying parties to relationships by antitrust authorities, courts of general jurisdiction and arbitration courts. It analyzes the content of the interdisciplinary institution of identification through the prism of Information Law and information security. The author makes some proposals for developing subject-specific Russian legislation considering the key task of ensuring information security of electronic communication in the digital economy and considers a new category "identification privacy".

Key words: information security, Information Law, institution of identification, legislation, case law, digital economy, identifier, personal data, facial identification, environment of trust, identification privacy.

For citation: *Naumov, V.B. (2019).* Information security in identification in the digital age: information law aspect // Gosudarstvo i pravo=State and Law, № 8, pp. 117–130.

The study was supported by the RFBR within the framework of the research project № 18-29-16013 "Research of conceptual approaches to the formation of the system of legal regulation of information security in the conditions of great challenges in the global information society".[1]

DOI: 10.31857/S013207690006736-1

The task and issues of identifying parties to relationships appeared a long time ago, with the emergence of large-scale social interactions. Those interactions required a legally valid way of identifying participants when people started to interact remotely. For example, in ancient history ambassadors or messengers would be sent, while in the Middle Ages, when banking relationships arose, promissory notes and related bank branches appeared in various European countries. In all of those cases the subjects and objects were in different locations where they had to be identified.

Identification[2] is one of the most ubiquitous life situations that have important social and legal meaning. Citizens of the Russian Federation encountered them both during the Soviet era and now, when in entirely different circumstances, from document checks to making transactions, today's parties to relationships are involved in identification processes. In the "ordinary" world a person regularly participates in one of the forms of identification: self-identification, when strangers present themselves to each other. Later they recognize (identify) them in communication by their physiological features and peculiarities, by their voice and even by their behavior and manners.

In the predigital age, in ordinary circumstances unrelated to accidents and violations of the law, identification was done primarily using identification documents. And initially the circulation of identification documents was directly or indirectly controlled by the state. Later on, non-state entities became involved in issuing them. In this area, the key issues were and continue to be focused on determining whether the documents and signatures used are authentic, and on combating forgery.

Everything changed radically with the advent of modern digital technologies. It is the digital age with its new technologies that has affected the overwhelming majority of branches and institutions of law. As the digital age evolves, existing institutions of law are being

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18–29–16013 «Исследование концептуальных подходов к формированию системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе».

[2] Without any claim to the truth, the author supposes that the term identification did not exist in antiquity, but the word "idem", meaning "the same", can be found in the Latin language (Latin-Russian Dictionary compiled by D.I. Fomitskiy, Feniks. 2001. P. 226), from which the concept of interest later came.

altered and new ones are being created. In the author's opinion, the latter also include the institution of identification, which already encompasses legal relationships that have similar objectives and incorporates a large number of accepted legal norms. Without setting the goal in this work of proving the author's hypothesis that the institution of identification became independent precisely within the Fourth Industrial Revolution and digital transformation of society, the state and economy, it is worth emphasizing that it is currently vital and important to regulate the processes of identifying parties to relationships, primarily individuals.

The large-scale adoption of technologies has made it possible to interact remotely with a person who is being identified, and individual users of the Internet and eGovernment services, online bank customers and online shoppers everywhere have appreciated this opportunity and have already become accustomed to the conveniences provided by technologies.

All of the above mentioned has spurred the development of statutory regulation of identification relationships in the digital environment. The fundamental feature of the relationships is that identification is done with the subjects and objects being located at a distance from one another. Yet old methods of identification using paperwork, dealing with notaries and even communicating in person can still be used in these legal relationships.

For example, one who uses different social networks rarely reflects on the fact that some of the networks' users have passed away and that their accounts are still available and often even "live" their own lives. The related problem of who inherits and gains access to these accounts appeared quite some time ago but has now become common. In some cases, network owners require that those interested in the account present a death certificate and original notary's acts. A number of cases result in litigation, and Google "since 2013 has invited the user him or herself to plan blocking or succession", for which purpose it has developed the special Google Inactive Manager[3].

Notwithstanding that example and many other life situations, in most cases business is now trying to use new technologies (e.g., facial recognition) to eliminate or minimize any in-person or document-based interaction. This is because user convenience is critical. However, the "price" of convenience and related risks could be quite high.

For example, quite recently the news agencies reported an outcome of poorly organized identification. According to the Fontanka.ru online publication, there was a road traffic accident in St. Petersburg in August 2019. One of the parties involved was driving a car sharing vehicle, was allegedly a minor and was driving without a driver's license. The publication reported that he had purchased an account for approximately RUB3.500[4] in order to use the car sharing service's vehicles.

It can be supposed that there will be more such cases where someone gets around the rules or technologies in order to be able to use one or another popular service and users are not accurately identified. In the case cited in St. Petersburg, there was a victim, and damage was caused to other road users. So, when and if a large number of people who are not entitled to drive start driving cars unchecked, there will be a widespread threat to public safety.

In order to eliminate this threat, the task of securing identification needs to be set across multiple disciplines. Legal problems and their solutions will be of key importance alongside technological and social problems. It must be connected with the development of the institution of information security, but may be considered even more broadly when the goal is to ensure the stability of electronic communications in the digital environment and the integrity of actions taken in that environment. This will provide the necessary level of trust and security in this area.

There are also related socio-political aspects to information security in identification. Given the triumphant progress of commercial technologies around the world, when there is as yet no convincing counterbalance to the "enthusiasm" over them, we need to understand that now it is extremely advantageous for digital business everywhere to identify all of its consumers and get the maximum amount of information about them in order to successfully sell goods and services to them at the right moment. Undoubtedly the state's interests in controlling citizens' actions that are taken for all kinds of different purposes – interests which have existed for centuries – are of considerable importance for developing the issues of secure identification. Another factor is related to the widespread phenomenon of fake identities (accounts) and fake news, when the security of society and the state will depend on how efficiently and quickly such accounts and news are identified.

Forming the basics of information law regulation of identification

Identification processes can be very diverse. They can have different objectives and tasks, result in identifying a person or identifying one or another person's

[3] See: *Uppit, O.* How Services and Social Networks Deal with Accounts of Deceased Users. [Online]: O. Uppit. Company Secret, 2018. URL: https://secretmag.ru/trends/whatsup/kak-servisy-i-socseti-obkhodyatsya-s-akkauntami-umershikh-polzovatelei.htm (accessed: 20.08.2019) (in Russ.).

[4] See: Carsharing Driver Responsible for Multi-Car Accident on Ligovskiy Was 16 Years Old. He Bought the Account [Online] // Fontanka.Ru. 2019. URL: https://m.fontanka.ru/2019/08/15/019/ (accessed: 20.08.2019) (in Russ.).

membership in a group of persons (recall here age labeling and regulation of alcohol and tobacco sales), or result in identifying only the devices people use. When users work on the Internet, they regularly find that information services use mini-puzzles to try to determine whether they are a robot or a human[5].

It is possible to categorize identification relationships in the digital environment by who is identifying whom, an individual or a legal entity; whether the state participates in the relationship; and whether government or non-government information resources and systems are used.

There is self-identification in this area, and trusted third parties (trusted parties, identification agents) are often used. From the technical perspective, the range of identification methods is quite broad. Enhanced digital signature technologies are often used in identification. Identification can consist of several levels and depend on a different number of identifiers with different information content, e.g., personal data.

There are many classes of identification relationships[6]. One of them, authentication, can be highlighted: if it is successful for the subject, then, based on authentication factors, the information system determines the subject's identifier.

Due to the wide range of legal relationships used and in which identification can be found, information law started to regulate it back in the mid-1990s. A vivid example could be the appearance in the old 1995 Federal Law "On Information, Informatization and Protection of Information" of the provisions of Articles 2 and 11 on personal data[7], which identified the then new category as information making it possible to determine an individual's identity. Other changes followed in other branches: from Information Law and Communications Law to Financial and Administrative Law[8].

At the current stage, there is interdisciplinary regulation of identification. Thus, it can be argued that this institution cuts across disciplines. Specialists are aware of the issues of identification in notarial activity, and the financial legislation defines simplified and ordinary identification separately[9]. Identification exists in the criminalistics system as the process of determining whether a specific object or person are identical based on a set of general and particular features by comparative examination to obtain forensic evidence[10].

It has also been enshrined in the civil legislation. For example, the provisions of the new version of Article 160(1) of the RF Civil Code enter into force on 1 October 2019. They have to do with observing the written form of a transaction, including one made using electronic or technical means: *"The requirement that there be a signature is considered met if any means is used that makes it possible to accurately identify the person who expressed their will. A law, other legal acts and the agreement of the parties may provide for a special method of accurately identifying the person who expressed their will"*[11].

The philosophy and sociology of law consider a related category: legal identity. N.V. Isayeva notes that *"the authors of European studies consider legal identity as the technological sequence of two stages: identity and identification. Initially there is identity with unique dynamic attributes granted at birth and stated in the registration record. Then, on the terms defined by the legislation of each state, there is identification as the processing of personal and unique data in biometric form (for example, in a national identity document or passport) when the person comes of age"*[12]. In her research this author also highlights an interesting phenomenon of *"identification management"*, interdisciplinary study of which (not only in the legal system) is worthy of separate attention.

We should be aware that in the near future identification will be both studied and regulated by other branches of law. For example, a group of academics led by I.L. Bachilo has noted that *"identifying sources of and the authors disseminating harmful information poses not only organizational, but also technological challenges, and also problems of how certain structures forming the Internet sector interact internationally"*[13]. They thereby outlined the international-law aspect of this phenomenon.

The 2013 amendments to the information legislation implementing a new information system in the country, The Unified System of Identification and Authentication, were a milestone in the evolution of

[5] See: CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart), the test Turing invented in 1950.

[6] See: *Naumov, V.B.* Scientific Approaches to the Classification of Types of Legal Identification in Information Law Relations // Proceedings of the Institute of State and Law of the Russian Academy of Sciences. 2016. No. 3. P. 104–115 (in Russ.).

[7] See: On Information, Informatization and Protection of Information [Online]: Article 609 of Federal Law No. 8 of 20 February 1995.– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[8] See: *Naumov, V.B.* Op. cit. (in Russ.).

[9] See: *Naumov, V.B., Braginets, A. Yu.* Information Law Aspects of the Remote Identification of Subjects in Financial Services // Information Law. 2016. No. 1. P. 13–19 (in Russ.).

[10] See: *Isayeva, N.V.* Legal Identity (a Legal Theory Study): Doctor of Legal Sciences Dissertation. 12.00.01 / Nina Valentinovna Isayeva.– Moscow, 2014 (in Russ.).

[11] On Amending Parts One, Two and Article 1124 of Part Three of the Russian Federation Civil Code [Online]: Federal Law No. 34-FZ of 18 March 2019.– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[12] On Amending Parts One, Two and Article 1124 of Part Three of the Russian Federation Civil Code [Online]: Federal Law No. 34-FZ of 18 March 2019. P. 112.– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[13] *Bachilo, I.L, Andryushchenko, Ye. A., Antopol'skiy, A.A., et al.* The Concept of the Information Code of the Russian Federation / Bachilo, I.L., ed. Moscow, 2014. P. 105 (in Russ.).

subject-specific legal regulation[14]. These amendments indirectly[15] provided definitions in the area of identification and determined the status of the government information system. The government information system was created primarily for the *"identification of information about participants of information interaction, including using qualified certificates of keys for verifying electronic signatures by comparing the identifier of a participant of information interaction or identifier of its information system entered in a common system, with information about that participant or about its information system contained in the respective basic information resource"*[16].

The legal regulation that has appeared does mention verification of the authenticity, accuracy and completeness of the information used, although separately, not in the unified system. This can be considered an important requirement for the identification process essentially defining the information security of identification for the subjects involved in it in the broad sense of the word.

The categories "identification" and "accuracy" [*dostovernost'*, also reliability)] were first used together in the 2014 legislative developments that supplemented the communications legislation: the law "On Communications" gained Article 44.1 "Distribution on a mobile wireless telecommunication network"[17], clause 1 of which states the following:

"Distribution [rassylka] on a mobile wireless telecommunication network (hereinafter also distribution) should be subject to obtaining the prior consent of the subscriber expressed by the subscriber taking actions uniquely identifying that subscriber and making it possible to reliably determine that the subscriber wants to receive the distribution".

Essentially, embedded in these provisions are ideas to ensure security in electronic communications, ideas making it possible to trust them: the subject is precisely identified and his or her expression of will by technical means is not doubted.

The legislation on identification has been actively developing in recent years. It is becoming more restrictive and increasing the burden on business in terms of legal risks (possible fines and blocking of services for failing to comply with lawmakers' requirements).

The year 2017 saw the introduction of Article 15.8 to Federal Law No. 149-FZ of 27 July 2006 "On Information, Information Technologies and Protection of Information". It prohibits anonymizers (services that make it possible to get around blocking and anonymously gain access to banned resources) from providing access to sites that disseminate information declared prohibited in the Russian Federation. It is anonymizers that are used, inter alia, to make it technically more complicated to identify the parties to relationships and difficult to identify the devices used by them to access the information. Since 2018 there has been a fine of between RUB800.000 and RUB1 million for failure by instant messaging service organizers to comply with user identification requirements (under Article 13.39 of the Administrative Offenses Code). This includes not only owners of messengers, but also, considered more broadly, other owners of services that provide chat services (the ability to correspond).

One of the important statutory acts in this area is RF Government Resolution No. 32 of 23 January 2006 (version of 25 October 2017) "On Approval of the Rules for Providing Data Transmission Communication Services", which sets forth a non-exhaustive list of means of identification, as long as they make it possible to accurately establish the information specified by the person.

Changes in the regulation of identification affect not only the digital area: requirements are changing for the identification of clients, beneficiaries and beneficial owners in financial and corporate relationships, and measures to monitor payments of unidentified individuals are also intensifying[18]. Another important point for many users [9]is that it will be prohibited to anonymously top up online wallets[19].

[14] See: On Amending the Federal Law "On Information, Information Technologies and Protection of Information" and the Federal Law "On Providing Access to Information about the Activities of the State Bodies and Local Authorities" [Online]: Federal Law No. 112-FZ of 7 June 2013.– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[15] In other words, without introducing definitions, but the meaning of the terms is implied by the provisions, for example, on how the government information system functions. We note that identification is defined only once in the federal laws: in Federal Law No. 115-FZ of 7 August 2001 (in the version of 26 July 2019) "On Counteracting Money Laundering and Financing of Terrorism" Article 3 states that "identification means all of the actions to establish the information specified by this Federal Law about clients, their representatives, beneficiaries and beneficial owners, and to confirm the accuracy of that information using originals of documents and/or duly certified copies and/or government and other information systems". The last words about information systems appeared recently, in connection with the amendments made at the end of 2017.

[16] Rules for Using the Federal State Information System "Unified System of Identification and Authentication in Infrastructure Supporting Information Technology Interaction of Information Systems Used to Provide State and Municipal Services in Electronic Form" [Online]: approved by Resolution of the RF Government No. 584 of 10 July 2013 (in the version of Resolutions of the RF Government No. 968 of 28 October 2013, No. 772 of 30 June 2018).– Available at 'ConsultantPlus" legal database (accessed: 20.08.2019).

[17] On Communications [Online]: Federal Law No. 272-FZ of 21 July 2014 – Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[18] See: On the National Payment System, Article 7(20) (effective date 15 Sept. 2019) [Online]: Federal Law No. 161-FZ of 27 July 2011 (version of 3 July 2019).– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[19] See: On Amending the Federal Law "On the National Payment System" and the Federal Law "On the Central Bank of the Russian Federation (the Bank of Russia)" [Online]: Federal Law No. 264-FZ of 2 August 2019 – Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

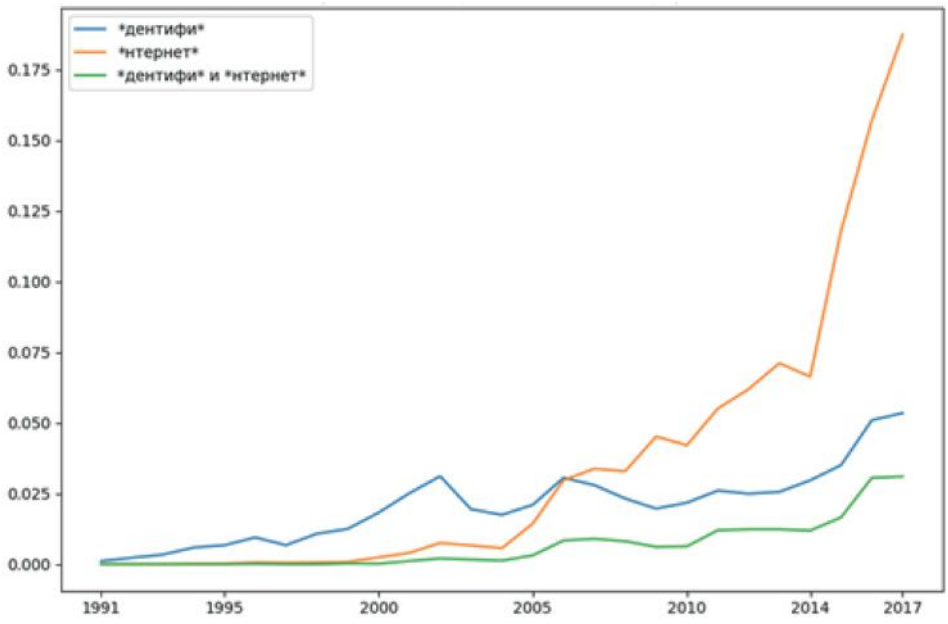

Fig. 1. Comparison of the frequency of mention of the words "identification" (*дентифи* in Russian), "Internet" (*нтернет*) and their collocations (*дентифи* and *нтернет*)[21]

Analysis of which branches of legislation and areas of regulation are seeing the most active appearance of provisions of the institution of identification shows that Internet-related legal relationships account for most of them.

This article includes researching the number of mentions of the terms "Internet" and "identification" in the text corpus of Russian Federation legal acts between 1990 and 2017. The public text corpus developed by D.A. Savel'yev was used for the study[20]. Only federal laws were selected from that corpus, and only legal acts newly adopted in the year indicated and amendments to previously adopted acts were considered (consolidated versions with amendments were not considered in order to avoid counting them twice).

The above graph shows that the number of documents mentioning the term "Internet" is on the rise: a rapid rise started in 2014 and collocation of the terms "Internet" and "identification" in the same document also grew during those years, together with an increase in the number of documents using the word "identification".

In absolute terms, the number of documents mentioning the term "Internet" grew from one in 1994 to 2.099 in 2017. The terms "identification" and Internet" in various forms of the words are mentioned together within a single document from 1996, but in 2017 the number of such documents grew to 348.

Individual sentences of the text corpus were also studied. The texts of the documents were first prepared by highlighting individual sentences from the texts of articles, clauses and other structural elements of the text. Of 5.5 million sentences, 234 sentences were found to contain these terms at the same time. Table 1 presents the trends in mentions of these terms by year.

In addition to the pattern identified above, it should also be acknowledged that the legal drafting of the documents in this area is deteriorating. There is also no unified system of terms for different branches of law and legislation for the same interdisciplinary institution of identification[22].

In addition to having a variety of discrepancies and gaps, the existing system of terminology has started to generate constructs that are difficult to subject to legal analysis. It is becoming popular in legislative work to include identification categories directly in the definitions of one or another technology. For example, two years ago Russia saw a new burst of progressive development of legislation on telemedicine. The telemedicine technologies themselves are now defined as follows: they are

[20] See: *Savel'yev, D.A.* On Creating and Using Text of the Russian Federation Corpus of Legal Acts as an Open Dataset // Law. Journal of the Higher School of Economics. 2018. No. 1. P. 26–44 (in Russ.). Information about the technology of this project, RusLawOD. URL: https://github.com/irlcode/RusLawOD/

[21] *Note*. The X axis plots the year the legal act was adopted, while the Y axis plots the ratio of the number of legal acts per year containing that word to the total number of documents adopted in that year. 200,502 documents obtained from the "Legislation of Russia" official legal information Internet portal were used for the calculation. The lines indicate any forms of the words "Internet" and "identification" and the words being found together within a single document.

[22] See: Naumov, V.B. Negative Patterns of the Formation of the Conceptual Apparatus in the Field of Internet Regulation and Identification // Information Law. 2018. No. 1. P. 32–39 (in Russ.).

Table 1

Trends in mentions of the terms "identification" and "Internet" by year

Year	Number
2003	1
2004	1
2005	2
2006	2
2007	1
2008	0
2009	1
2010	1

Year	Number
2011	7
2012	22
2013	16
2014	27
2015	26
2016	36
2017	48

"information technologies enabling healthcare providers to interact with one another, with patients and/or their legal representatives remotely; identification and authentication of individuals' data, documentation of the actions they take during conferences, consultations and remote medical monitoring of the patient's health"[23].

This approach and similar ones where the definition of technologies includes processes that are also not fully regulated or are regulated differently in branches of legislation should be eliminated in further legislative development. On the other hand, one can understand the idea of the initiative's developers: the price of an error and, in general, social responsibility in the field of identification is high. For example, issues of identification are some of the current issues in foreign research on the quality of healthcare services. For example, in the US, analyzing extensive statistics on various ways of interacting with patients, they suggest using ideas of constantly identifying patients at each step of healthcare and service[24].

Federal Law No. 482-FZ of 31 December 2017 "On Amending Certain Legislative Acts of the Russian Federation" is the latest milestone in the development of legislation on identification. It laid the foundations for the possibility of using biometric personal data to identify individuals remotely.

Since 30 June 2018 the Federal Law "On Information, Information Technologies and Protection of Information" has regulated the use of information technologies for remote identification of Russian Federation citizens using their biometric personal data. Interactive remote authentication and identification of individuals who are clients of lending institutions has been permitted since early 2018 in order to conclude agreements with those institutions.

The essential novelty in the legislation was the category of the *"unified biometric system"*, a *"unified information system of personal data supporting the processing, including collection and storage, of biometric personal data, their verification and transmission of information on the degree to which they match the provided biometric personal data of a Russian Federation citizen"* (Article 14.1 of the law).

An individual's data wind up in the system after the individual has been personally identified (in his or her presence) and with his or her consent, after which the data are processed for identification purposes. It is the competent employees of government authorities or organizations who place the data in the system and they are signed with an enhanced encrypted and certified digital signature.

Article 14.1(18) of the Law "On Information, Information Technologies and Protection of Information" makes it possible in the cases contemplated by federal laws to identify a Russian Federation citizen without the citizen being personally present by providing government authorities and organizations with information from the Unified System of Identification and Authentication and information about the degree to which the biometric personal data of the person provided match his/her biometric personal data contained in the unified biometric system.

Encryption tools must be used in the second case, when the Internet is used; however, the individual is given the right to choose whether to opt-out of using these tools or not. An opt-out should be informed and the person should be warned of the risks related to opting out.

The only exceptions to this situation (Article 14.1(20) of the Federal Law) are cases when an individual uses

[23] On Amending Certain Legislative Acts of the Russian Federation on Issues of the Application of Information Technologies in Healthcare [Online]: Article 3 of Federal Law No. 242-FZ of 29 July 2017 – Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[24] See: Patient Identification Errors [Online] // The Health Technology Assessment Information Service (HTAIS). 2016. URL: https://www.ecri.org/Resources/HIT/Patient%20ID/Patient_Identification_Evidence_Based_Literature_final.pdf (accessed: 20.08.2019).

a mobile telephone, smart phone or tablet computer to provide their biometric personal data. In that case, remote identification should be denied if encryption tools are not installed on them.

An important methodological aspect should be noted here. The latter two constructs related to freedom of choice and an injunction against using mobile equipment are nothing else but a fragment of the idea of ensuring identification is secure in the broad sense of the term.

Without having other specific provisions on secure identification, unfortunately, from the legal drafting perspective this law seems more like a statutory act or an instruction; however, it does outline a regulatory vector that is intended to secure subject-specific legal relationships despite the convenience of the technology itself for business and the state.

As part of this milestone, a package of statutory regulations disclosing detailed requirements and rules on biometric identification was adopted in the summer of 2018. So, according to RF Government Resolution No. 772 of 30 June 2018, the following biometric personal data of an individual who is a citizen of the Russian Federation will be recorded in the unified biometric system: *"data of an image of the person's face obtained with the help of photo and video devices; the person's voice data obtained with the help of sound recording devices"*[25].

Ideally, the legislation on identification should be technically neutral in order not to be dependent on identification methods and algorithms that regularly appear. There are very few examples of this so far, but if we analyze Russian and foreign experience, this objective has not been achieved.

From the technical perspective, the biometric personal data mentioned above may not actually serve to accurately identify someone in real life.

For example, the idea of manipulating photographs and videos has been around for a long time. The plot of the 1994 film *Forrest Gump* has the main character, played by actor Tom Hanks, meet with President John F. Kennedy, who is convincingly portrayed on screen. This scene must have demanded a lot of technical resources from the filmmakers of that day. However, now the technologies are becoming more perfect and less expensive, which means that people who are ignorant of the nuances of image processing algorithms can to this. It has even led to the coining of a special new term, "DeepFake"[26], and special freely distributable software has become available. It both replaces images of a person's face in an existing video and, using special algorithms to detect and generate poses, creates footage of actions that don't exist. It looks as if a real person has made those movements and taken those actions.

Given how popular ideas of widespread video surveillance and recording and biometric identification by images are, including when provisions on them are introduced into the legislation, real-time fake videos will be a serious blow for these ideas. Without using special hardware and software, neither systems nor people will be able to distinguish between what is genuine and what has been generated, most often for illegal or dishonest purposes.

However, even without dishonest generation or substitution of video information, the world has taken notice of the fact that convenient and developing technologies can contribute to the violation of human rights and interests. A case in point here is the United States, where the US Senate has introduced a bill on commercial facial recognition privacy[27]. The bill prohibits the use of facial recognition technology without obtaining the affirmative consent of the end user. However, the law does not cover legal relationships in state administration and security.

Similar ideas can also be found in other countries of the world and they are also supported by Russian researchers. For example, V.V. Yarkov and I.G. Rents assert that "the use of biometric data to identify individuals in civil transactions is generally not allowed, as it violates privacy"[28].

In May 2019 technology publications spread the news that the San Francisco Board of Supervisors banned biometric identification use by the police and other entities with oversight authority. The decision passed by an eight to one vote and makes San Francisco the first major US city to have a tool used by many police officers to search for petty crime and terrorism suspects.

The San Francisco Board of Supervisors Ordinance[29] amending the state's Administrative Code is

[25] "On approving the procedure for processing, including collection and storage, of the parameters of biometric personal data for the purposes of identification, the procedure for placing and updating biometric personal data in the unified biometric system, and requirements to information technologies and hardware intended for processing biometric personal data for identification purposes" (see: Registered with the Ministry of Justice of Russia on 4 July 2018, No. 51532) [Online]: Order of the Russian Communications Ministry No. 321 of 25 June 2018.– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[26] Which can be translated into Russian as kachestvennaya poddelka (quality fake).

[27] See: The Commercial Facial Recognition Privacy Act [Online] // Congress. 2019. URL: https://www.congress.gov/bill/116th-congress/senate-bill/847 (accessed: 20.08.2019).

[28] Yarkov, V.V., Rents, I.G. The Validity of the Principles of Notaries in the 21st Century: New Challenges // Law. 2019. No. 7. P. 42 (in Russ.).

[29] See: Administrative Code – Acquisition of Surveillance Technology [Online] // The Committee on Information Technology. 2019. URL: https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061–4D87–4A94–9AB3-CB113656159A (accessed: 20.08.2019).

intended to restrict not only facial recognition technologies, but also all "surveillance technologies"[30]. The Ordinance will also restrict the local police from transmitting information to federal agencies (e.g., to immigration and customs control). However, the restrictions will not apply at San Francisco International Airport, where the federal agencies have jurisdiction. There, they will be able to freely use facial recognition systems and biometric scanners at their discretion.

The State of Illinois adopted its Artificial Intelligence Video Interview Act at almost the same time[31]. The act provides that an employer that asks applicants to record video interviews and uses an artificial intelligence analysis of applicant-submitted videos shall notify each applicant in writing before the interview that an artificial intelligence program may be used to analyze the applicant's facial expressions and consider the applicant's fitness for the position. The employer must also explain before the interview how the program works and what characteristics it uses to evaluate applicants, and obtain written consent from the applicant to be evaluated by the artificial intelligence program.

The Illinois act provides that an employer may not share applicant videos with third parties, except with persons whose expertise or technologies are necessary in order to evaluate an applicant's fitness for a position. Upon request from the applicant, the act states that employers, within 30 days after receipt of the request, must delete an applicant's interviews and instruct any other persons who received copies of the applicant video interviews to also delete the videos, including all electronically generated backup copies.

So far, Russia's regulatory framework does not consider such social technology issues; however, the number of conflicts and open issues directly or indirectly related to identification is growing.

Patterns in identification law enforcement

In recent years, the Federal Antimonopoly Service has had to deal with identification issues in the Russian Federation every so often. Mostly this is related to cases over the legality of distributing promotional marketing, which in recent decades has plagued individuals' text messages and e-mails.

Here, since Article 18 of the Federal Law "On Advertising" places the burden of proving consent to the distribution was obtained on advertising distributors, in administrative proceedings it is advertising distributors who must prove how they identified the subscriber or user and obtained consent from them. Russia's Federal Antimonopoly Service authorities build their logic on the above-mentioned rule and para. 15 of Resolution of the Plenum of the RF Supreme Arbitration Court No. 58 of 8 October 2012 "On Certain Issues of the Practice of Application by the Arbitration Courts of the Federal Law 'On Advertising'", where it is stated that as the Federal Law "On Advertising" "does not specify how and in what form the subscriber's prior consent to receive advertising on telecommunication networks should be obtained, the subscriber's consent can be expressed in any form sufficient to identify the subscriber and confirm he or she wants to receive advertising from a specific advertising distributor".

The electronic nature of communication makes it difficult to prove this. Thus, the FAS Office for the Yaroslavl Region stated in its Decision of 21 December 2017 in case No. 04–01/13–17 that "evidence sufficient to identify the subscriber and confirm that the subscriber expressed his will to receive advertising directly from a specific advertising distributor was not submitted to the case file. Registration of the subscriber's number on the http://beget.com/ru/free-hosti№ g website does not make it possible to determine that it was precisely the individual who is that number's subscriber who registered and made an expression of will to receive the advertising".

It is important to bear in mind that in FAS Russia's practice of hearing such cases the claimants almost always assert that they did not consent to receiving advertising text messages or e-mails and it is almost impossible for advertising distributors to prove otherwise. This is a rare situation in life of a commercial entity being the "weak party". Perhaps it did get the user's consent to receive advertising, but it is unable to prove it convincingly in FAS proceedings.

The FAS Office for Moscow made an interesting finding about identification in its decision of 5 December 2017 in case No. 3–18–120/77–17: "If the text of the information does not contain any reference to means of identification making it possible to identify its recipient, it can be said that the information is targeted at the general public, regardless of how many people received the information. The advertising text does not contain the personal data of the person who is the intended target of the information being distributed".

The regulator's finding was important for qualifying that advertising does not have restrictions on its distribution based on its content.

In both cases the use of trusted communications or an environment of trust where all those involved interact with predetermined parties to the relationship could solve the issue of who was identified as a party to the relationship. But the author does not think it is possible to organize them for the now commonly used text or e-mail distributions. And, importantly, it does not seem

[30] The San Francisco Board of Supervisors decision defines quite a wide range of items as surveillance technology: cell site simulators, automatic license plate readers, gunshot detection hardware and services, video and audio monitoring and/or recording technology, etc.

[31] The Artificial Intelligence Video Interview Act [Online] // General Assembly. 2019. URL: https://legiscan.com/IL/bill/HB2557/2019 (accessed: 20.08.2019).

necessary for this respected but gradually aging insecure means of communication. There is also an opposing view: in the summer of 2019 a group of senators in the Federation Council introduced draft amendments to Article 10.1 of the Federal Law "On Information, Information Technologies and Protection of Information" regarding mandatory identification of e-mail users by mobile telephone number[32]. The draft law would prohibit the transmission of messages from persons who have not been identified.

An interesting and fair finding on the scope of identification to identify the sender of messages has been made, but in litigation with other facts. In case No. A32–28069/2016 the courts tried to ascertain who sent a claim over non-performance of a contract, and to whom, and found the following: *"The receipt or sending of a message using an e-mail address known as the e-mail of the entity itself or the office e-mail of the entity's competent employee evidences that those actions have been taken by the entity itself, unless and until it has proven otherwise. The respondent's argument that the claim was sent not from an e-mail address belonging to the claimant cannot be admitted by the appellate court, as the respondent should have known that the claim had been received precisely from the claimant and not from another person when it received a message regarding remedying defects referencing the contract and the name of the customer"*[33].

Now almost standard for the arbitration [*arbitrazh*] courts is the logic of considering relationships using a qualified e-signature where the qualified e-signature of the sender of a document (Article 160(2) of the RF Civil Code) is proof that a party to a contract made the documents (e.g. an offer or acceptance) electronically (Article 434(2) of the RF Civil Code). It can be considered that additional proof that the document comes from the party to the contract is not required if it is not disputed that the signature was lawfully used.

It is also obvious that in proceedings the parties are entitled to rely not only on e-signature technologies used, but also on the e-mail correspondence itself whether or not its status, or how the parties conduct it, were determined in advance, for example, by concluding an agreement on how they would exchange documents. It is fair to believe here that if an e-mail is sent from the e-mail address of a person's employee participating in the correspondence, that person has taken the actions unless proven otherwise.

An essential factor for its subsequent evaluation by the court could also be the practice that has evolved in the electronic exchange of documents by parties to a future conflict. The argument of the Arbitration Court of the Urals Circuit in one of the arbitration cases seems progressive. It states that *"a business custom arose by exchanging electronic messages to e-mail addresses allowing them to identify each addressee, including by the content of the messages"*[34].

Of procedural value could be another fact which the Presidium of the Intellectual Property Court mentioned two years ago when summarizing its case law: *"difficulty in identifying the sender and addressee may not allow such correspondence to be considered relevant to the dispute being examined, as it is not possible to correlate such information with the parties in dispute and the relations between them. However, if both 'corresponding' parties confirm the fact that it exists, such evidence may be deemed relevant if there are no other obstacles"*[35].

As regards electronic messaging, to qualify advertising distribution relationships the court, just as FAS Russia before it, summarized the endemic problem of ordinary electronic communications as the impossibility of uniquely identifying who is sending out one or another piece of information.

It is also difficult to determine who is distributing or providing information on social networks. The courts of general jurisdiction also encounter this problem. For example, a group was blocked on the VKontakte social network and its administrators asked the court to unblock it because it was found that spam about joining the group was sent from fake accounts and it was sent from the same IP address as the group's administrator[36].

The difficulty of proving who owns an account on an information system could be very important for the party concerned. This is confirmed by the emerging case law involving online games, when people devote their

[32] See: State Duma Finds Conflict with the Constitution in Klishas' New Draft Law [Online] // Interfax. 2019. URL: https://www.interfax.ru/russia/670148 (accessed: 20.08.2019).

[33] Resolution of the 15th Arbitration Court of Appeal of 29 September 2017 and Resolution of the Arbitration Court of the North-Caucasus Circuit of 12 January 2018 No. F08–10440/2017 in case No. A32–28069/2016 [Online].– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[34] Resolution of the Arbitration Court of the Urals Circuit of 13 February 2018 in case No. A60–23408/2015 [Online].– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[35] An Information Note Prepared Based on the Results of Summarizing the Case Law of the Intellectual Property Court as a Court of First Instance and Cassation, Taking into Account the Practice of the Supreme Court of the Russian Federation on Some Issues that Arise when Evaluating Evidence Containing Information Posted on the Internet [Online]: Resolution of the Presidium of the Intellectual Property Court No. SP-23/24 of 14 September 2017.– Available at "ConsultantPlus" legal database (accessed: 20 Aug. 2019). Resolution of the Intellectual Property Court of 3 October 2016 in case No. A40–138017/2013 [Online].– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[36] See: Ruling of the Primorsk Kray Court of 5 April 2016 in case No. 33–3158/2016 [Online]. E-filing of procedural documents. (2017). [Online] // Primorsk Kray Court. 2017. URL: https://kraevoy–prm.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=8983579&delo_id=5&new=5&text_number=1 (accessed: 20.08.2019).

time and money playing the games and find that everything they have "accumulated" or "earned" in the game disappears. This happened with a gamer from Siberia. The court said that "there is no evidence in the case file that the claimant has a contractual relationship with the defendant. Given these circumstances, Individual 1's claims to restore access to the R2 Online game unaltered and keeping all of the game results and gambling valuables as at the date access was restricted should not be granted, nor should the claims for compensation of moral harm and a fine stemming from the subject matter of the dispute be granted"[37].

Considering the situations mentioned above and the example of online games, one could argue that issues of identification are universal for the modern digital environment and can be found varieties of its areas. This is also fair to say of the computer game industry because, as V.V. Arkhipov correctly argues, "virtual worlds present the full range of Internet-law issues"[38], and at the same time "virtual worlds can be used as models of the real world and as a space for social experimentation"[39]. Issues of identification in the gaming environment also make it possible to view issues of the limits of the law's effect in a new light. For example, in the context of the possible creation and use of non-existent users' profiles and well-known situations where fake accounts are used. These issues can be corelated to the broad understanding of the well-known set of issues surrounding the "magic circle" (a well-established term denoting the conventional boundary of virtual reality in which real-life law supposedly does not apply). Some researchers interpret them as universal legal issues in the context of the medial turn; issues that are not limited to games alone[40].

It should be noted that groundbreaking technologies in the digital economy affect not only the identification of humans using video images or in computer games. Identification of individuals by processing big data is certainly a pressing problem. The processing could happen without people being notified, or even when information that cannot identify someone if used in small amounts is collected and processed. Big data present huge opportunities for business and the state; they essentially open up new management horizons for them. A 2019 case study by the Russian Presidential Academy of National Economy and Public Administration of the development of public administration in the digital age correctly notes that *"the variety of sources of data that are needed in decision-making, the dynamic development of new technologies for the collection and processing of information require that a flexible system for regulating data management processes be developed and a framework definition of the term 'big data' be devised that would eventually make it possible to use new types of information for public administration"*[41].

It can be supposed that, thanks to big data, in the near future the state will have new, expansive capabilities to identify groups of people and individuals. It is appropriate to ask here whether the existing scope of privacy rights and guarantees protects them.

Knowledge of the sciences that will help to formulate the necessary decisions should influence the content of the norms of the interdisciplinary institution of identification and the principles of creating regulations here.

There will be a similar situation where the use of artificial intelligence technologies will depend on knowledge beyond the humanities. Of course, there is a major difference: the artificial intelligence realm could see the appearance of objects capable of acting like a human and this will require a rethinking of the entire legal system in general and identification in particular to determine whether something is "alive / not alive". Russian academics are already shaping the range of substantive ideas in their research. For example, together with A.V. Neznamov, the author proposes to develop a principle of conscious interaction resulting in a human's informed consent to the use of stand-alone artificial intelligence systems[42].

The task of ensuring information security of identification in the digital environment

Particular attention was paid to issues of identification in regulation and public administration when the ideology behind the "Digital Economy of the Russian Federation" program was formed[43] in 2017. For the first time at the state level the program raised the issue of

[37] Decision of the Leninskiy District Court of the City of Tyumen of 10 November 2015 in case No. 2–9870/2015 [Online].– Available at "ConsultantPlus" legal database (accessed: 20.08.2019); Judicial proceedings and court decisions [Online] // Leninskiy District Court of the City of Tyumen. 2015. URL: https://leninsky–tum.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=3473596&delo_id=1540005&new=0&text_number=1 (accessed: 20.08.2019).

[38] *Arkhipov, V.V.* Virtual Law: Main Problems of the New Direction of Legal Research // University News. Jurisprudence. 2013. No. 2 (307). P. 103 (in Russ.).

[39] Ibid. P. 106.

[40] See: *Arkhipov, V.V.* Cybersport Law: Myth or Reality? // Law. 2018. No. 5. P. 80–92 (in Russ.).

[41] Digital Future of Public Administration by Results / Ye.I. Dobrolyubova, V.N. Yuzhakov, A.A. Efremov, etc. Moscow, 2019. P. 69 (in Russ.).

[42] See: *Naumov, V.B., Neznamov, A.V.* // The Model Convention on Robotics and Artificial Intelligence: Approaches to Identification and Security Issues. In the collection: Dynamics of Information Security Institutions. Legal Challenges. Collection of Research Papers. T.A. Polyakova, V.B. Naumov and E.V. Talapina, ed. 2018. P. 136 (in Russ.).

[43] See: "Digital Economy of the Russian Federation" program approved by Order of the RF Government No. 1632-r of 28 July 2017.– [Online].– Available at "ConsultantPlus" legal database (Accessed: 20.08.2019). Note: the document was repealed on

how important identification issues are for the state. The issue was brought to light through the set of challenges the country faces as part of digital transformation:

"The development of Russia's digital economy is hampered today by new challenges and threats, primarily ... the problem of protecting human rights in the digital world, including during identification (correlation of a person with his/her digital image), integrity of the user's digital data, and the problem of ensuring individuals' trust in the digital environment..."[44].

A corresponding task was created for this threat (item 1.1 of the Program): the task of creating the legal conditions to form a single digital environment of trust that will provide participants in the digital economy with means of "trusted digital remote communications"[45] in order, among other things, to remotely confirm a person's identity to take legally binding actions and various methods of identifying and authenticating people.

What needs to be regulated in this area, and how? Ideally, first of all, there needs to be a single set of terms integrating the concepts of "identification", "authentication", "registration", "recognition", "certification", "login", "user definition", "identifier use", etc., currently found in very different contexts, into a single hierarchical pyramid of terms for the identification process.

Worthy of particular attention here is the definition of the general term "identifier". It is used to determine whether one or another category (a party to a relationship (subject), an object, process or a combination thereof) matches the information about him or it in an information system. And a subject or object can have a few or even many identifiers. An identifier is of course information that can be open and public, or access to and exchange of this information may be restricted. For example, everyone is aware of such public identifiers as tax identification numbers, which are used to solve a number of identification tasks in the business and tax areas. On the other hand, logins and passwords are not public identifiers[46].

The legislation must set forth which subjects are involved in identification. It must determine their legal status and mutual rights and obligations. Legal mechanisms and requirements for protecting individuals' rights at the time of identification must be proposed, and the judicial and administrative jurisdiction of identification-related disputes must be specified in the legislation.

The trusted third party (or agent) should be highlighted as a type of subject. It is becoming more and more desirable to involve a trusted third party in legal relationships, and it is the trusted third party who provides identification services for a person who wants to do identification but does not have the technologies or resources for this.

What needs to be proposed is a balanced system of identification principles and related requirements as to when simplified identification can be used in certain types of legal relationships and when ordinary identification can be used. In the latter case, additional organizational and technical solutions should also be used to keep identification secure. It seems appropriate to introduce a new (third) category in addition to the first two categories: "enhanced identification". It could be used in areas that are economically important for individuals and for security, for example, in making real estate transactions.

It seems important to introduce a new type of information system to the legislation: the identification information system. In this case, the existing definition of the unified system of identification and authentication that appeared in 2013 would become a part of it. It is the requirements to organizing and operating this system, conditions for accessing it and keeping its information secure that will support the general goal of secure communications in which identification of subjects will ensure the necessary level of trust in digital communications.

It will also be important when developing subject-specific legislation to consider that identification may extend across borders.

In the race for technological innovation it is important not to forget that the technologies aren't yet reliable enough and the traditional identification processes cannot be entirely discontinued, nor can persons, in particular, individuals, be required to use electronic (digital) identification without alternatives. Moreover, in our opinion, the new requirements in this area need to be changed and created in such a way that new laws are introduced for a number of types of legal relationships gradually considering people's poor technological culture and literacy (even among young people) as well as external factors related to the need to evaluate the extent to which new technologies, in addition to being convenient, will harm existing socioeconomic processes.

According to the regulatory development action plans, the development of new special remote identification legislation should be completed in the autumn

---

12 February 2019 in connection with the publication of Order of the RF Government No. 195-r of 12 February 2019.

[44] On Approval of the "Digital Economy of the Russian Federation" program (repealed) [Online]: P. 12 of Order of the RF Government No. 1632-r of 28 July 2017 – Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[45] Ibid.

[46] A person's name is also an identifier. It is very interesting when reviewing the research on the customs of different peoples to see how some of them made the use of a name taboo or set rules and restrictions on using a name in public and private life.

of 2019[47]. The development of special legislation will make it possible to talk about developing the content of such a legal institution as the institution of identification. At the same time, it is important to bear in mind that if it is possible to create a regulatory framework for trusted communications in the near future, then an important step will have been made in ensuring parties to legal relationships are securely identified in the digital age.

Identification privacy as a new category of Information Law

To summarize the analysis done, it seems important to consider legal relationships in the area of identification and to set corresponding tasks in policymaking and law enforcement based on the task of keeping the information in these relationships secure.

This means security in the broad sense of the word:

— for the person being identified, in order not to violate his or her rights and interests;

— for the person doing the identification, so that the identification algorithms and solutions used do not become known.

And it is important for the identification to deliver the result sought: accurate identification of the person involved in the relationship or other facts related to the actions of the person involved in the identification.

This task should be a key one for developing a legal model for regulating and creating comprehensive legislation.

Keepi in mind that there is a kind of "unity and struggle of opposites" of the legal relationship considered here, especially for individuals who are being identified. T.A. Polyakova uses an appropriate term to describe this struggle in analyzing information security relationships: the dichotomy of action and reaction[48], where, on the one hand, the principle of personal privacy is set against the requirements and interests of identification.

In this regard, we need to answer the question of whether it is possible to introduce a right for an individual to consent or refuse to be identified. Another important factor follows from this and it determines whether the identification is secure for the person being identified: whether the person is informed of the purposes and, possibly, of the terms of the identification process.

It should be considered that the state's policy on anonymity and identification in the information field in Russia and the world changed at the start of this decade. There is a trend in Russia for the state and society to seriously start thinking about how privacy protections can be abused, that overall state control has increased, legislation introducing a mandatory identification requirement, and, in a number of cases, prohibiting anonymous interaction, has started to appear.

This article proposes to introduce a new category in information law in the system of the interdisciplinary institution of identification: identification privacy. Its objective would be to secure identification in the broad sense of ensuring that identification algorithms are legal and reliable and achieving accurate identification results.

It is important that the algorithms used be confidential: the person organizing the identification or the person providing identification services must be entitled to keep the identification technologies secret.

Another essential feature of the new category is connected with the fact that both any information received and processed in the course of identification and the results must be used only for the purpose for which the processing was done. This has a certain similarity to the purposes for which personal data are processed, but, if personal data are not available (for example, in incomplete identification or processing of big data), it seems necessary to also keep that information secret. Otherwise there is a risk of doing identification of a person without having informed them or obtained their consent.

And, finally, a third feature of the category is to keep the very fact of identification secret, unless otherwise implied by the circumstances and requirements for organizing the identification process, a contract or a law.

The following analogy can be used to understand and further discuss the new category academically. This privacy will essentially be a combination of norms similar to those of another type of privacy: communication privacy (given that communication privacy has a quite limited area of application in the legislation on communications with its special subjects, communications service providers) and the confidentiality of information about technologies, sensitive personal data and other information that could be used to identify subjects.

* * *

In conclusion, it should be noted that while the task of securing identification in the broad sense is being addressed, liability should also be introduced for incorrect or incomplete identification if a misleading result has caused any adverse consequences.

[47] See: On Approval of the "Digital Economy of the Russian Federation" program (repealed) [Online]: P. 74 of Order of the RF Government No. 1632-r of 28 July 2017 – Available at "ConsultantPlus" legal database (accessed: 20.08.2019).

[48] See: *Polyakova, T.A.* Digitization and Synergy of Legal Support for Information Security // Information Law. 2019. No. 2. P. 3 (in Russ.).

REFERENCES

1. Administrative Code – Acquisition of Surveillance Technology [Online] // The Committee on Information Technology. 2019. URL: https://sfgov.legistar.com/View.ashx? M=F&ID=7206781&GUID=38D37061–4D87–4A94–9AB3-CB113656159A (accessed: 20.08.2019).
2. An Information Note Prepared Based on the Results of Summarizing the Case Law of the Intellectual Property Court as a Court of First Instance and Cassation, Taking into Account the Practice of the Supreme Court of the Russian Federation on Some Issues that Arise when Evaluating Evidence Containing Information Posted on the Internet [Online]: Resolution of the Presidium of the Intellectual Property Court No. SP-23/24 of 14 September 2017.– Available at "ConsultantPlus" legal database (accessed: 20 Aug. 2019). Resolution of the Intellectual Property Court of 3 October 2016 in case No. A40–138017/2013 [Online].– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).
3. *Arkhipov, V.V.* Cybersport Law: Myth or Reality? // Law. 2018. No. 5. P. 80–92 (in Russ.).
4. Digital Future of Public Administration by Results / Ye.I. Dobrolyubova, V.N. Yuzhakov, A.A. Efremov, etc. Moscow, 2019. P. 69 (in Russ.).
5. *Arkhipov, V.V.* Virtual Law: Main Problems of the New Direction of Legal Research // University News. Jurisprudence. 2013. No. 2 (307). P. 103, 106 (in Russ.).
6. *Bachilo, I.L, Andryushchenko, Ye. A., Antopol'skiy, A.A., et al.* The Concept of the Information Code of the Russian Federation / Bachilo, I.L., ed. Moscow, 2014. P. 105 (in Russ.).
7. Carsharing Driver Responsible for Multi-Car Accident on Ligovskiy Was 16 Years Old. He Bought the Account [Online] // Fontanka.Ru. 2019. URL: https://m.fontanka.ru/2019/08/15/019/ (accessed: 20.08.2019) (in Russ.).
8. Decision of the Leninskiy District Court of the City of Tyumen of 10 November 2015 in case No. 2–9870/2015 [Online].– Available at "ConsultantPlus" legal database (accessed: 20.08.2019); Judicial proceedings and court decisions [Online] // Leninskiy District Court of the City of Tyumen. 2015. URL: https://leninsky – tum.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=3473596&delo_id=1540005&new=0&text_number=1 (accessed: 20.08.2019).
9. "Digital Economy of the Russian Federation" program approved by Order of the RF Government No. 1632-r of 28 July 2017.– [Online].– Available at "ConsultantPlus" legal database (Accessed: 20.08.2019). Note: the document was repealed on 12 February 2019 in connection with the publication of Order of the RF Government No. 195-r of 12 February 2019.
10. *Isayeva, N.V.* Legal Identity (a Legal Theory Study): Doctor of Legal Sciences Dissertation. 12.00.01 / Nina Valentinovna Isayeva.– Moscow, 2014 (in Russ.).
11. *Naumov, V.B.* Negative Patterns of the Formation of the Conceptual Apparatus in the Field of Internet Regulation and Identification // Information Law. 2018. No. 1. P. 32–39 (in Russ.).
12. Patient Identification Errors [Online] // The Health Technology Assessment Information Service (HTAIS). 2016. URL: https://www.ecri.org/Resources/HIT/Patient%20ID/Patient_Identification_Evidence_Based_Literature_final.pdf (accessed: 20.08.2019).
13. *Naumov, V.B.* Scientific Approaches to the Classification of Types of Legal Identification in Information Law Relations // Proceedings of the Institute of State and Law of the Russian Academy of Sciences. 2016. No. 3. P. 104–115 (in Russ.).
14. *Naumov, V.B., Braginets, A. Yu.* Information Law Aspects of the Remote Identification of Subjects in Financial Services // Information Law. 2016. No. 1. P. 13–19 (in Russ.).
15. *Naumov, V.B., Neznamov, A.V.* // The Model Convention on Robotics and Artificial Intelligence: Approaches to Identification and Security Issues. In the collection: Dynamics of Information Security Institutions. Legal Challenges. Collection of Research Papers. T.A. Polyakova, V.B. Naumov and E.V. Talapina, ed. 2018. P. 136 (in Russ.).
16. *Polyakova, T.A.* Digitization and Synergy of Legal Support for Information Security // Information Law. 2019. No. 2. P. 3 (in Russ.).
17. Registered with the Ministry of Justice of Russia on 4 July 2018, No. 51532) [Online]: Order of the Russian Communications Ministry No. 321 of 25 June 2018.– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).
18. Resolution of the 15th Arbitration Court of Appeal of 29 September 2017 and Resolution of the Arbitration Court of the North-Caucasus Circuit of 12 January 2018 No. F08–10440/2017 in case No. A32–28069/2016 [Online].– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).
19. Resolution of the Arbitration Court of the Urals Circuit of 13 February 2018 in case No. A60–23408/2015 [Online].– Available at "ConsultantPlus" legal database (accessed: 20.08.2019).
20. Ruling of the Primorsk Kray Court of 5 April 2016 in case No. 33–3158/2016 [Online]. E-filing of procedural documents. (2017). [Online] // Primorsk Kray Court. 2017. URL: https://kraevoy – prm.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=8983579&delo_id=5&new=5&text_number=1 (accessed: 20.08.2019).

21. *Savel'yev, D.A.* On Creating and Using Text of the Russian Federation Corpus of Legal Acts as an Open Dataset // Law. Journal of the Higher School of Economics. 2018. No. 1. P. 26–44 (in Russ.). Information about the technology of this project, RusLawOD. URL: https://github.com/irlcode/RusLawOD/

22. State Duma Finds Conflict with the Constitution in Klishas' New Draft Law [Online] // Interfax. 2019. URL: https://www.interfax.ru/russia/670148 (accessed: 20.08.2019).

23. The Artificial Intelligence Video Interview Act [Online] // General Assembly. 2019. URL: https://legiscan.com/IL/bill/HB2557/2019 (accessed: 20.08.2019).

24. The Commercial Facial Recognition Privacy Act [Online] // Congress. 2019. URL: https://www.congress.gov/bill/116th-congress/senate-bill/847 (accessed: 20.08.2019).

25. *Uppit, O.* How Services and Social Networks Deal with Accounts of Deceased Users. [Online]: O. Uppit. Company Secret, 2018. URL: https://secretmag.ru/trends/whatsup/kak-servisy-i-socseti-obkhodyat-sya-s-akkauntami-umershikh-polzovatelei.htm (accessed: 20.08.2019) (in Russ.).

26. *Yarkov, V.V., Rents, I.G.* The Validity of the Principles of Notaries in the 21st Century: New Challenges // Law. 2019. No. 7. P. 42 (in Russ.).

Authors' information

NAUMOV Victor B. –
PhD in Law, associate Professor, leading researcher of the Information Law and international information security sector of the Institute of State and Law of the Russian Academy of Sciences; 10 Znamenka street, 119019 Moscow, Russ**ia**