вая природа и проблемы применения в современной России // Уголовно-исполнительная система: право, экономика, управление. 2012. № 3.

10. Конституция Российской Федерации. Комментарий / Под общ. ред. Б.Н. Топорнина, Ю.М. Батурина, Р.Г. Орехова. - М.: Юрид. лит-ра, 1994.
11. Марогулова И.Л. Законодательные проблемы амнистии и помилования // Журнал российского права. 1998. № 1.
12. Молчанов П.В. Административная амнистия для нарушителей правил дорожного движения. // Право и государство: теория и практика. 2009. № 10 (58). С. 104.
13. Салпагаров М.У. Амнистия как межотраслевой юридический институт и некоторые проблемы ее реализации. // Перспективные направления развития современной юридической науки. Сборник статей международной научно-практической конференции, посвященной 20-летию юридического факультета и 75-летию Петрозаводского государственного университета. 2015.
14. Скуратов Ю.И., Чурилов С.Н., Грудинин Н.С. Государственная политика в сфере амнистии и помилования в Российской Федерации: тенденции и противоречия // Криминологический журнал Байкальского государственного университета экономики и права. 2015. Т. 9, № 1.
15. Таганцев Н.С. Уложение о наказаниях уголовных и исправительных 1885 года – СПб. 1904.
16. Щербакова Е.В. Проблемы реализации института амнистии при освобождении граждан РФ от административной ответственности // Реформы и власть: особенности и функционирование гражданского общества: межвуз. науч. сборник. Воронеж, 2010. Вып. 5.
17. Проект нового Кодекса Российской Федерации об административных правонарушениях - https://regulation.gov.ru/projects#npa=102447 (дата обращения: 18.09.2020).

Aleksei G. Deineko
Kosygin State University of Russia, The Department of civil law and public law, Associate Professor, Ph. D. in Law, (115035, Moscow, Sadovnicheskaya, 52/45. alexey-deyneko@mail.ru; SPIN: 8899-7709 AuthorID: 704121)

ANONYMITY AS THE INHERENT NATURE OF CYBERSPACE

Keywords: *legal theory; information law; anonymity; privacy; cyberspace; Internet; deanonymization; national security.*

Abstract: *This article aims to explore the legal nature of the concept «anonymity» of the subjects of relations that occur in information-telecommunication networks. Anonymity will be considered in two aspects: as the inherent nature of cyberspace and as one of the most important subjective rights in the structure of studied relationships. Also an interdisciplinary approach will be applied to this concept.*

The article also analyzes the first results of amendments to the information legislation in terms of identification of users of cyberspace, adopted in 2017, as well as new legislative initiatives in this area, currently being considered in the State Duma of the Federal Assembly of the Russian Federation.

Problem statement

The concept of anonymity, which does not leave from news feeds in recent years, can be called one of the symbols of the modern cyberspace. Within a few years, this concept has passed from the vocabulary of secret services and coders into everyday speech. This is largely due to the activities of the regulators to “bringing order” on the Internet. Despite the fact that anonymity is often perceived

by the legal community as a phenomenon that does not need to be explained, in many ways it remains to be *terra incognita*.

The format of the article, unfortunately, does not allow us to analyze all the features of the phenomenon of anonymity in cyberspace that is why we review the key technical and legal aspects of this phenomenon. We have repeatedly drawn attention to the fact that cyberspace has become a fundamentally new sphere of law, and anonymity, in turn, is its organic property, along with cross-border and interactivity[70]. This feature of cyberspace, coupled with the development of wireless public access networks and technologies for changing (masking) IP-addresses, has been worried Russian lawmakers for many years. In 2016, German Klimenko, adviser to the President of Russian Federation on Internet issues, called anonymity the most serious problem of the Internet and de facto recognized that it was impossible to solve it quickly[71]. Some attempts have already taken place in Russian practice in terms of introducing mandatory identification of users of public Wi-Fi networks[72], and they can hardly be called effective. In recent years the legislator has made a number of steps, which, however, have not led to a full solution to this problem[73].

July 29, 2017 Russian President Vladimir Putin has signed two laws directly related to the issue of cyberspace

[70] See for example, *Deineko A.G.* (2017). Avtorskoe pravo v kiberprostranstve: monografiya [Copyright in cyberspace: monography] Moscow: Yurlitinform. P. 15. (in Russ.).

[71] Interview with G. Klimenko (2016) [online]. Izvestia [News]. Available at: https://iz.ru/news/608118 [Accessed November 1, 2019].

[72] Art. 1 Decree of the Government of the Russian Federation of august, 12, 2014 No. 801 «On amendments to certain acts of the Government of the Russian Federation» // Svod zakonov Rossijskoj Federacii [Russian Code of Laws], august 25, 2014. No. 34. Art. 4662.

[73] See for example, *Naumov V.B.* (2018). Problemy razvitiya zakonodatel'stva ob identifikacii sub"ektov informacionnyh otnoshenij v usloviyah cifrovoj ekonomiki [Problems of development of legislation on identification of subjects of information relations in the digital economy] // Trudy Instituta gosudarstva i prava RAN [Proceedings of the Institute of State and Law of the RAS]. 13 (4). P. 131.

anonymity: Federal law No. 241-FZ[74] and Federal law No. 276-FZ[75]. Many experts note that the draft laws related to the regulation of cyberspace tend to have ultra-short (from two weeks to one month) terms of discussion in the lower house of Parliament[76].

Law 241-FZ, also known as the "Messengers Law", amended Federal law of July 27, 2006 No. 149-FZ "On information, information technologies and information protection " (hereinafter - "Information Law"), fixing a new concept for the Russian law system: "organizer of an instant messaging service". The definition is formulated so vaguely that it includes not only well-known messengers - WhatsApp, Viber, Telegram, etc., but also, for example, social networks. For such organizers, the Messengers Law establishes the obligation to identify users of services using the mobile operator's subscriber number "in accordance with the procedure established by the Government of the Russian Federation", which came into force in May 2019[77], as well as the obligation to ensure the confidentiality of transmitted electronic messages. In other words, messenger users will be identified through the SIM cards that they use to access the Internet, but in return they will receive a

[74] Federal law of July 29, 2017 No. 241-FZ «On amendments to articles 10-1 and 15-4 of the Federal law "On information, information technologies and information protection"» (hereinafter – 241-FZ). Avalaible at: Ofitsialniy Internet-portal pravovoi informatsii [Official Internet-portal of law information] URL: https://pravo.gov.ru, ID: 0001201707300031. [Accessed November 1, 2019].

[75] Federal law of July 29, 2017 No. 276-FZ «On amendments to the Federal law "On information, information technologies and information protection"» (hereinafter – 276-FZ). Avalaible at: Ofitsialniy Internet-portal pravovoi informatsii [Official Internet-portal of law information] URL: https://pravo.gov.ru, ID: 0001201707300002. [Accessed November 1, 2019].

[76] Interview with head of NGO «Roscomsvoboda» A.Kozluk (2017) [online]. «Afisha.Daily». Avalaible at: https://daily.afisha.ru/technology/5885-v-rossii-blokiruyut-vpn-i-tor-svobodnomu-internetu-konec [Accessed November 1, 2019].

[77] Decree of the Government of the Russian Federation of October, 27, 2018 No. 1279 «On approval the Rules for identifying users of the Internet by the organizer of the instant messaging service» (came into force May 5, 2019) // Svod zakonov Rossijskoj Federacii [Russian Code of Laws], November 12, 2018. No. 46. Art. 7043.

guarantee of confidentiality of the transmitted data. There is no answer to the question of what to do with users who purchased a SIM card without entering a passport data (which is absolutely legal today) or use a SIM card issued to another person.

Law No. 276-FZ, also known as the "Anonymizers Law" amended the Information Law by prohibiting the use of software that allows users to change (mask) their IP-addresses, reducing the possibility of their identification to zero. To legally define anonymizers, the legislator used a very cumbersome construction: "information-telecommunication networks and information resources, through which access to information resources and information-telecommunication networks is provided, access to which is restricted on the territory of the Russian Federation"[78]. At the same time, «*information resources*» mean a website on the Internet and (or) a website page on the Internet, an information system, or a computer program. The authors of the 276-FZ paved a shaky bridge between information and copyright law, given that information has not been the object of civil rights for many years[79], but computer programs are[80]. Thus, new concept «information resources» combines two different groups of objects: site, site page, information system (information law) and computer programs (copyright law). Thus, the existing discussion in the Russian jurisprudence about the legal nature of information and related concepts is even more complicated.

It should be noted that the 276-FZ does not establish a total ban on the use of anonymizers, it is only prohibited to use them to overcome Roskomnadzor's blocking. Owners of information-telecommunication networks and information resources that are used to overcome blocking, are required to "ensure compliance with the ban" on access to blocked Internet sites, but the law does not explain how they should do this. At the same time, for non-compliance, is provided a responsibility in the form of restricting access to the owner's software and hardware, regardless of the owner's national jurisdiction. It is obvious that foreign owners of anonymizers, having received a Roskomnadzor's notification, will not eagerly comply with it, but rather will create a "mirror" of a potentially blocked site.

In general, this legal construction looks like a matryoshka doll - it is possible that the Roskomnadzor registry will be supplemented with sites that were blocked for providing tools to access blocked sites, etc. Users of cyberspace, in turn, will create information resources to overcome the blocking of information resources intended to bypass the blocking of Internet sites. It should be noted that in the explanatory note to the federal law draft No. 195446-7[81], which was the prototype of 276-FZ, is noted that the practice of blocking web sites, which has developed since 2012, revealed the insufficient effectiveness of the blocking mechanism.

New beginnings

Despite the noted width of the thesaurus of 241-FZ, 2019 was marked by another resonant initiative related to the deanonymization and addressed to e-mail users. Apparently, legal practice has revealed the incorrect application of the Messenger Law to e-mail users, which prompted

[78] Art. 15.8 of Information Law.

[79] Art. 128 of the Civil Code of the Russian Federation (Part 1) of November, 30, 1994 No. 51-FZ // Svod zakonov Rossijskoj Federacii [Russian Code of Laws], December, 5, 1994. No. 32. Art. 3301.

[80] P. 1 art. 1259 of the Civil Code of the Russian Federation (Part 4) of December, 18, 2006, No. 230-FZ // Svod zakonov Rossijskoj Federacii [Russian Code of Laws], December, 25, 2006. No. 52 (Part 1), art. 5496.

[81] Federal law draft No. 195446-7 «On amendments to the Federal law "On information, information technologies and information protection" (in terms of clarifying the procedure for restricting access to information resources)» // Available at: https://sozd.duma.gov.ru/bill/195446-7 [Accessed November 1, 2019].

senators A. Klishas, L. Bokova, A. Bashkin, A. Karlin to introduce a draft law that extends the obligation to identify e-mail users. Moreover, we are talking about two draft laws with identical names: the first one was introduced on July 23, 2019 under the No. 760029-7[82] and is currently cancelled, the second draft law was introduced by the same senators on October 8, 2019 under the No. 808655-7[83] and, most likely, it will be the basis for future amendments to the Information Law.

In the explanatory notes to both draft laws it was noted that the changes made in 2017 to the Information Law, according to the developers, "had a positive impact on the security of the Russian Federation." The necessity of the identification of e-mail users is due to the growth of false messages about the threat of terrorist acts. Federal law draft No. 760029-7 regulated in detail actions of the organizers of e-mail services in relation to users of such services and messages transmitted by them, while the Federal law draft No. 808655-7 has only obligate them to «restrict users abilities». Also, a draft law No. 808655-7 proposes to remove the term "instant" from all legal constructions with the "instant messaging service", thereby extending the effect of the Messenger Law to e-mail services. Such novelties are unlikely to be working themselves until the relevant amendments are made to the Decree of the Government of the Russian Federation of October 27, 2018, No. 1279, which is still action in pilot mode[84]. In addition,

[82] Federal law draft No. 760029-7 «On amendments to the article 10-1 of Federal law "On information, information technologies and information protection" (in terms of establish email service organizer's responsibilities)» // Available at: https://sozd.duma.gov.ru/bill/760029-7 [Accessed November 1, 2019].

[83] Federal law draft No. 808655-7 «On amendments to the article 10-1 of Federal law "On information, information technologies and information protection"» // Available at: https://sozd.duma.gov.ru/bill/808655-7 [Accessed November 1, 2019].

[84] This is confirmed by numerous journalists experiments, proved that after the entry into force of this Decree, any one can still purchase a SIM card without presenting an ID, installing any messengers, adding funds to the account balance and without any risk of being identified – *AA*.

it may be necessary to adopt a special legal act, established the procedure (method) for filtering messages containing prohibited information by e-mail services, as well as by a regulator that is not yet known.

Thus, we can state the legislative "trend" of recent years — the desire of the legislator to "deanonymize" cyberspace by any ways. This trend is likely to lead to an "exodus" of users to foreign service providers, who are unlikely to obey with Russian law requirements. A significant number of legal entities and public authorities that provide their employees (officials) corporate email addresses fall under the scope of the proposed laws. The question of identifying email addresses belonging to legal entities, state and local government bodies, as well as their various divisions (departments, services, etc.) remains unanswered.

As for the Russian owners of information-telecommunications networks and information resources that qualified as anonymous technologies, since none of them is able to control how they are used by end users (especially if we are talking about computer programs), the most reasonable action for them in terms of risks minimizing is to delete such a network or information resource.

Supporters of access to the Internet "by passport" often call anonymity as a clear threat to national security, arguing that it helps to commit crimes — from hacking social networks accounts to large-scale hacker attacks. However, the Doctrine of information security, approved by the President of Russia in December 2016, does not call anonymity as one of the threats to our country's information security[85].

[85] The doctrine of information security of the Russian Federation, approved by Decree of the President of the Russian Federation of December 5, 2016 No. 646 // Svod zakonov Rossijskoj Federacii [Russian Code of Laws], 12.12.2016. No. 50. Art. 7074.

This is because anonymity, like any other technological tool, cannot be used solely for the purpose of causing harm. For example, anonymous technologies are successfully used for the state protection of victims, witnesses and other participants of criminal proceedings, by journalists in "hotspots", as well as in the practice of transnational corporations for the safe transfer of information. The authors of the draft law (Federal law No. 195446-7) in an explanatory note to it also pointed to "a wide range of possibilities for their legal application". In this regard, one of the key disadvantages of 276-FZ, in our opinion, is the lack of differentiation between the legal and illegal use of anonymous technologies. SMS and other mobile communications are often used when commiting crimes (and even terrorist attacks), but this does not mean that these technologies should be also banned.

The most common technologies for providing anonymity in cyberspace can be divided into three groups. The first group includes so-called VPN services[86], which now have formed a large market with paid access to these services. It seems that 276-FZ is directed against Internet sites that offer to "buy a VPN". However, blocking a site that offers a paid access to VPN, will not affect the performance of the VPN service itself, and users who previously paid for access will be able to continue using it. It should be noted that, according to our estimates, the number of advertising offers for the purchase of VPN services over the past two years has not changed significantly.

The second group of technologies includes various add-ons for Internet browsers (Google Chrome, Opera, Mozilla Firefox, etc.) that allow users to change their own IP-address by one click. These applications are usually free of charge and are most convenient for users. It seems that such add-ons were what the legislator meant when he used the term "computer programs". In this case, we can expect bans of using of software-add-ons, and in the worst case, the entire Internet browser. Finally, the third group includes TOR-technologies[87], the perspective of blocking which is most doubtful.

We can agree with the forecast of analysts of the Internet media "Medusa" that law enforcement bodies will focus their efforts primarily on the first two groups, since they are the most popular and easiest to use[88]. The Chinese experience of fighting with TOR, where the state has spent huge technological and financial resources to block the output nodes of TOR networks, is disappointing for supporters of blocking. The developers "taught" the system to "build bridges" through hidden repeaters, and as a result, TOR networks became more perfect, and huge state resources were wasted. In fact, the China state has invested significant resources in improving the technology that was going to be banned.

Certain doubts arise when referring to the question of the time limits of the legislative novels. As we know, *lex prospicit, non respicit*, but in this case we can talk about an example of the hidden retroactive force of the law. At the time of creating special add-ons for Internet browsers or sites that offer VPN services, such actions of developers and users were absolutely legal. 276-FZ does not contain any reservations that it does not apply to information resources created before its adoption, which means that it

[86] VPN (*Virtual Private Network*) – generic name for technologies, provide one or more network connections (a logical network) on top of another network (for example, the Internet). It should be noted that VPNs can be used not only for anonymous data transfer, but also for other purposes, including access to the Internet. For more information, see URL: https://ru.wikipedia.org/wiki/VPN [Accessed November 1, 2019].

[87] TOR (*The Onion Router*) – software (as well a proxy system) that allows to establish a secure anonymous network connection. Like a VPN, it can be used for "peaceful purposes". For more information, see URL: https://ru.wikipedia.org/wiki/Tor [Accessed November 1, 2019].

[88] «Meduza», July, 3, 2017 // Available at: http://meduza.io/feature/2017/07/03/vlasti-sobirayutsya-zablokirovat-vpn-i-anonimayzery-a-eto-voobsche-vozmozhno [Accessed November 1, 2019].

may be quite real that developers will be responsible for the technology or program that they created 5 or 10 years ago. At the same time, users who paid for a VPN service or installed software before the 276-FZ entry into force, theoretically, should not be responsible for the use of anonymous technologies.

The constitutional dimension of anonymity

For a more complete analysis of the legal nature of anonymity in cyberspace, it necessary to consider it not only from the standpoint of information law, but also in conjunction with the right to privacy, established by part 2 of article 23 of the Constitution of the Russian Federation. The Constitution of the Russian Federation, as we know, establishes an open list of possible means of communication, through which personal correspondence can be carried out, and also speaks about the only possible way for restricting the right to privacy – a court decision. In this regard, anonymity should be considered as the most important technological tool aimed performing the constitutional right of everyone to privacy. A person who uses anonymous technologies to visit unbanned Internet sites is reasonably based on the legality of their actions. Thus, a complete ban on the anonymous technologies in cyberspace is impossible due to its obvious unconstitutionality.

Anonymous technologies are on a par with encryption technologies that allow you to secure payments and correspondence in cyberspace, but at the same time are not identical them. In this regard, soon it will become possible to establish the right to secure Internet access in the constitutions of modern countries and international legal acts. At the same time, today we can name possible components of the right to anonymity. Experts of the «Russian center for digital rights protection» identify the following components of this right:

- the right to anonymous web surfing (searching for information on the web) and anonymous sending of personal messages (including via messengers);
- the right to anonymous posting (publication of information in the network);
- the right to anonymous payments (including the use of cryptocurrencies);
- the right to create and distribute works anonymously[89].

We can generally agree with the proposed classification, if we take into account that these rights can also be implemented using encryption technologies, i.e. encrypted data transmission, rather than anonymous. In support of the position on the need to establishing these rights, the «Russian center for digital rights protection» experts refer to the practice of higher courts in foreign legal systems (in particular, the Supreme Court of the US[90] and the ECHR[91]), and to the positions of international organizations (the UN Human rights Council[92], the Council of Europe, etc.).

Analyzing these examples, we can draw two conclusions from the legal positions of these bodies. First, courts and international organizations require states to respect the desire of citizens to access the Internet anonymously and not to obstruct it. Secondly, these bodies assume that the right to anonymity cannot be absolute and may be subject to reasonable, justified and lawful restrictions, as well

[89] Available at: https://habrahabr.ru/company/digitalrightscenter/blog/329050 [Accessed November 1, 2019].

[90] A selection of decisions of the Supreme Court of US in cases related to anonymity and freedom of speech on the Internet // "Electronic Frontier Foundation". Availaible at: https://www.eff.org/updates?type=case [Accessed November 1, 2019].

[91] See for example, ECHR cases K.U. vs. Finland, № 2872/02, December 2, 2008, Delfi vs. Estonia, № 64569/09, October, 10, 2013, etc..

[92] UN Human rights Council resolution No. A/HRC/32/L.20 «The promotion, protection and enjoyment of human rights on the Internet». June 27, 2016 // Available at: https://undocs.org/A/HRC/32/L.20 [Accessed November 1, 2019].

as other constitutional rights. After all, even in those developed legal systems where the death penalty is prohibited, the most important constitutional right – the right to life — is still a subject to certain restrictions – for example, through the necessary self-defense or (less often) legalizing euthanasia. In addition, in some cases, identification of a person may be obligated for the realization of other constitutional rights – for example, when a citizen applies for state and municipal services in electronic form. In these conditions, it is not necessary to talk about the right to anonymity, since the law on personal data protection comes into play. It should be noted that Russian legal experts draw attention to the conceptual and terminological discrepancy between the legislation on identification and on personal data protection[93].

There is hardly find any convincing arguments that anonymous payments to charitable foundations (even from foreign sources) pose any threat to national security. However, such threat may arise in the case of anonymous funding of political organizations, which means that the right to anonymous payments should still be subject to constitutional restrictions. The question of whether to restrict the right to publish information anonymously in cyberspace deserves a separate discussion and is beyond the scope of this article.The problem of the limits to the realization of the right of everyone to privacy is relevant for western legal systems. The debatable issue is the limits of restricting this right by the state when it is necessary for fight against terrorism and extremism. In this case, we are talking about the state interference in the personal life of law-abiding citizens, not the terrorists (extremists). In cases where the object of interference is the personal life

[93] *Naumov V.B.* (2018). Nauchnye podhody k klassifikacii vidov pravovoj identifikacii v informacionnyh pravootnosheniyah [Scientific approaches to classification of types of legal identification in information legal relations] // Trudy Instituta gosudarstva i prava RAN [Proceedings of the Institute of State and Law of the RAS]. 55 (3). Pp. 104-115.

of a potential criminal, the law on operational search activity enters into the case, allowing in such cases to obtain a court sanction. A clear illustration of this trend is the USA Patriot Act[94] adopted in the United States after the September 11, 2001 attacks, which expanded the powers of law enforcement agencies to monitor citizens, including in cyberspace. Adopted as a temporary measure, this law was in effect for 14 years, until its provisions were significantly relaxed in 2015. One of the pushes to soften the provisions of the USA Patriot Act was the report of the US Department of justice on the ineffectiveness of this law.

Unfortunately, the Russian legislator did not take into account the experience of overseas colleagues and in 2016 Russia adopted the infamous "Yarovaya package"[95], which established the obligation for all information mediators to decrypt messages transmitted by users (text, voice, video, photo and other messages) and store them for 6 months. The "Yarovaya package" is related to the USA Patriot Act with a common goal (fighting against terrorism) and a large resonance that both of these acts caused in the Internet community. It is still too early to assess the effectiveness of these laws, but even today we can see a serious burden on telecom operators and information mediators in the costs of purchasing and operating special equipment. This has already led to increase in the cost of communication services provided on the territory of Russia. In addition, with regard to the "Yarovaya package", the doubts remain about its compliance with the articles 23,

[94] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, October, 26, 2001, № 107-56. // Available at: https://congress.gov/107/plaws/publ56/PLAW-107publ56.pdf [Accessed November 1, 2019].

[95] The «Yarovaya package» includes two laws, but in this case we are talking about Federal law No. 374-FZ of July 6, 2016 "On amendments to the Federal law "On countering terrorism" and certain legislative acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety" // Avalaible at: Ofitsialniy Internet-portal pravovoi informatsii [Official Internet-portal of law information] URL: https://pravo.gov.ru,. ID: 0001201607070016 [Accessed November 1, 2019].

24 of the Constitution of the Russian Federation (in part on the necessity of a court decision to restrict the right to privacy and the need for a person's consent to collect, store and use information about his private life).

The law should be economical

Questions about the feasibility of restricting the right to use anonymous technologies have not only a legal, but also an economic dimension. In this regard, it seems necessary to apply a law-economical analysis, to estimate the costs and benefits of making the legislative decisions.

First of all, anonymity itself can be considered as an economic category. It is the opposite of individualization, which has value for the product, including for the Internet user, if he himself acts as a product, exploiting its popularity. This does not mean that anonymity has no economic value or has a negative value. If the user does not make money on their own identity (for example, by blogging), anonymity is an economically valuable benefit for them, the loss of which they will perceive as a damage. Anonymity has an even greater economic value when transferring confidential information between commercial companies, as pointed above. Thus, the state, depriving individuals and legal entities from economic benefits (anonymity), or to be more precise, limiting their ability to use such benefits, is forced to bear organizational, technical and financial costs. The costs should also include the risks of incorrect enforcement, since the mentioned laws and draft laws are not perfect in terminology.

Richard Posner, a professor at the University of Chicago School of law, provides the following formula for an economic and legal analysis of the problem of limits and restrictions on freedom of speech in the United States:

$$pH / (1+d)^n + O \geqslant B - A$$

where **H** means the harm that public statements are likely to cause with probability **p**, **O** – the offensiveness caused

by such statements, **B** – the benefits of allowing dubious statements by the state, **A** – the costs of imposing bans, and $(1+d)^n$ are the discount rate for future costs or profits compared to the present. In other words, the state should prohibit questionable statements if and only if the expected harm from the statements, discounted based on their probability and time of occurrence, exceeds the amount of benefits from them and the costs of prohibiting them[96].

If we extrapolate this formula (without indicator **O**) to the anonymity problem, we will conclude that the actions of the state to deanonymize the Internet will be effective only when the expected benefit from these restrictions exceeds all possible costs incurred by the state and society. With regard to the "fight against VPN", it should be considered, that the costs incurred by Russian IT companies will be higher than at foreign competitors, since the risks of them to suffer from the actions of Roskomnadzor should be assessed lower. This may create an economically paradoxical picture, when the state actually imposes additional burdens on domestic IT companies instead of helping them to improve their competitiveness in the world market.

If, as a result of restrictions on the use of VPN in the Runet, the technological chain of transmitting confidential information of any business entity is disrupted, this will be a danger signal for the entire market. These costs are directly related to the concept of the "digital economics"[97], the need to build which speak Russian leaders, and at the same time, they are the most difficult to calculate.

[96] *Pozner R.* (2017) Rubezhi teorii prava [Frontiers of law theory] / translate from Eng. by *Kushnareva E.*, under the ed. *Odintsova M.* Moscow: Publishing house of Higher school of economics. (in Russ.). P. 76.

[97] Passport of the National project "Digital economics of the Russian Federation" (approved by the Presidium of the Council to the President of the Russian Federation for strategic development and national projects, protocol No. 7 of June 4, 2019) // Available at: https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf [Accessed November 1, 2019].

If we look to the left side of the above formula, we will see that prof. Posner's allows us to abstract from unnecessary moral and ethical aspects of the anonymity problem. If the "Yarovaya package" calls the fight against terrorism among its main goals, then based on a purely moral assessments, it will not be difficult to conclude that even one prevented terrorist attack will equal billions costs to decrypt and store the correspondence of users of cyberspace. From the point of view of law-economic analysis, we will be talking about a very high potential harm (**H**), which can occur with a relatively small probability **p**, which in turn will allow us to raise the question of other, possibly more effective options for allocating financial costs for the fight against terrorism.

Summing up the attempt at law-economics analysis of the phenomenon under consideration, it should be notes the high potential value of this method, which in the future could be used for the preparation of financial and economic justifications for draft of legal acts, including mentioned in this article.

Some conclusions

Anonymity, as one of the organic properties of cyberspace, cannot be called an absolutely harmful phenomenon. In some cases, the use of anonymous technologies benefits both individuals and society as a whole by increasing the security of data transfer in cyberspace. However, it is necessary to distinguish between the anonymous and cryptographic technologies, since in the first case, the devices that transmit information are depersonalized, and in the second case, the transmitted information itself is encrypted.

Anonymity should be considered as one of the key mechanisms for implementing the constitutional right to privacy. This right is not absolute, so its recognition by states does not exclude the possibility of minor restrictions on the use of anonymous technologies (for example, in terms of anonymous payments to prevent the financing of terrorist or extremist organizations). At the same time, anonymous communication in cyberspace should not be prohibited to users, for whom government bodies do not have reliable information about their involvement in socially dangerous acts.

Russian legislator, having adopted new laws requiring messenger operators to identify all users and prohibiting the use of VPN, continued the trend to deanonymization of cyberspace. The Internet community perceives anonymity as a benefit that it does not want to lose, and in response to each legislative novel develops new technologies to circumvent new prohibitions.

Looking at the anonymity problem from the point of view of the theory of benefits and costs allows us to make a conclusion that it is necessary to analyze law-economic aspects of legislative initiatives related to the regulation of cyberspace. Legislation in this area should be based not only on the legislator's ideas about "reasonable, good, eternal", but also on the laws of the market, and achievements of economic science. The ratio of costs and benefits, that the state and society are ready to incur from the adoption of a new law, should become as integral element of the legislative process as the legal examination of draft laws.

However, we cannot rule out a scenario where the further development of technology will seriously change the concept of anonymity. If one person uses a single mobile device to access the Internet at home, at work, and anywhere in the world by simply connecting to public networks, then this device (through the contract concluded with the seller of the device) will be the legal basis for identifying the user. If we recall the forecasts of futurists predicting the appearance of microchips integrated into the human body and connected to the Internet, it becomes

obvious that with each round of technological progress, the legislator will face more and more complex tasks.

REFERENCES:

1. *Deineko A.G.* (2017). Avtorskoe pravo v kiberprostranstve: monographiya [Copyright in cyberspace: monography] Moscow: Yurlitinform. (in Russ.).
2. *Naumov V.B.* (2018). Nauchnye podhody k klassifikacii vidov pravovoj identifikacii v informacionnyh pravootnosheniyah [Scientific approaches to classification of types of legal identification in information legal relations] // Trudy Instituta gosudarstva i prava RAN [Proceedings of the Institute of State and Law of the RAS]. 55 (3). Pp. 104-115.
3. *Naumov V.B.* (2018). Problemy razvitiya zakonodatelstva ob identifikacii sub'ektov informacionnyh otnoshenij v usloviyah cifrovoj ekonomiki [Problems of development of legislation on identification of subjects of information relations in the digital economy] // Trudy Instituta gosudarstva i prava RAN [Proceedings of the Institute of State and Law of the RAS]. 13 (4). Pp. 125-150.
4. *Pozner R.* (2017) Rubezhi teorii prava [Frontiers of law theory] / transl. from Eng. by *Kushnareva E.*, under the ed. *Odintsova M.* Moscow: Publishing house of Higher school of economics. (in Russ.).

ПЕШИНА Инна Юрьевна,
Национальный исследовательский университет «Высшая школа экономики», факультет права, старший преподаватель (109028, Москва, Б.Трехсвятительский пер., 3; тел.: +7495-772-9590; email:ipeshina@hse.ru)

ШАБЛИНСКИЙ Илья Георгиевич,
Национальный исследовательский университет «Высшая школа экономики», факультет права,доктор юридических наук, профессор, член Кафедры ЮНЕСКО НИУ ВШЭ (109028, Москва, Б.Трехсвятительский пер., 3; тел.: +7495-772-9590; email: ishablin@hse.ru)

ПРОБЛЕМА СВОБОДЫ ВЫРАЖЕНИЯ МНЕНИЙ В РЕШЕНИЯХ ЕСПЧ (в рамках анализа конкретного решения)

Ключевые слова: *Европейский Суд; свобода выражения мнения; права журналистов; репутация публичного лица; утверждения о фактах; оценочные суждения.*

Аннотация: *Противостояние свободных средств массовой информации и государства в лице его институтов является серьезной проблемой как для России, так и для многих других европейских государств. Решения Европейского Суда по правам человека по жалобам журналистов и средств массовой информации на нарушения статьи 10 Европейской Конвенции о защите прав человека и основных свобод напоминают национальным судам о необходимости обеспечения свободы массовой информации в соответствии с внутренним законодательством и принятыми на себя государствами международными обязательствами. В решении по делу «Скудаева против России» Европейский Суд подчеркнул, что национальным судам следует искать баланс между свободой слова и свободой средств массовой информацией, с одной стороны, и правом публичного лица на честь и достоинство, с другой. Суд также напомнил о важности различения информации о фактах и оценочных суждений журналиста в связи с*