ЖУРНАЛИСТИКА
ИСТОРИЯ И ТЕОРИЯ СМИ

JOURNALISM
HISTORY AND THEORY OF MEDIA

The Transformation of the Idea of Internet Freedom in the XXIst Century

Ivan I. Zassoursky[ID], Nataliia D. Trishchenko[ID]✉

Lomonosov Moscow State University,
9 Mokhovaya St, Moscow, 125009, Russian Federation
✉ trishchenko.nataliia@yandex.ru

Abstract. The article analyzes the theoretical approaches that have developed in relation to the issues of control and freedom of the Internet space, including copyright regulation and its gradual transformation as the digital environment develops and changes. Special attention is given to the values underpinning the principles of regulation are determined. If initially the dominant notion was that the Internet would ensure humanity a new free world, then later the discourse shifted to much less optimistic views and topics the issue of network regulation, technical and legal restrictions, censorship and data protection. Most recent academic literature is devoted to the practical side of the issue, and the issue of values has faded into the background. As a result, the discussion has lost significant context: issues of freedom and human rights in the Internet environment, discussion of what is really important for society – security or the absence of restrictions, the problem of users' trust in the state and platforms.

Keywords: internet regulation, copyright, code

Conflicts of interest. The authors declare that there is no conflict of interest.

Article history: submitted: January 29, 2021; accepted: March 11, 2021.

Трансформация представлений о свободе интернета в XXI веке

И.И. Засурский, Н.Д. Трищенко

Московский государственный университет имени М.В. Ломоносова,
Российская Федерация, 125009, Москва, ул. Моховая, д. 9
✉ trishchenko.nataliia@yandex.ru

Аннотация. В статье анализируются теоретические подходы, сложившиеся в отношении вопросов контроля и свободы интернет-пространства, в том числе регулирования в сфере авторского права, их постепенная трансформация по мере развития и изменения условий развития цифровой среды. Особое место в рассмотрении проблемы занимают ценности, в соответствии с которыми определяются принципы регулирования. Если изначально доминирующие позиции занимали представления о том, что благодаря интернету человечество получит новый свободный мир, то в дальнейшем дискурс сместился к гораздо менее оптимистичным взглядам и темам – вопрос регулирования сети, техническим и правовым ограничениям, цензуре и защите данных. При этом основное внимание в свежих научных источниках уделяется именно практической стороне вопроса, а ценностная – уходит на второй план. В результате за рамками дискуссии оказывается значимый контекст: вопросы свободы и прав человека в интернет-среде, обсуждение того, что является действительно важным для общества – безопасность или отсутствие ограничений, проблема доверия пользователей к государству и платформам.

Ключевые слова: интернет-регулирование, авторские права, код

Introduction

The growth of the Internet has significantly enhanced the role of media in the life of society, causing academics from a variety of fields to pay attention to the processes of mediatization. Initially, academic research was primarily concerned with the technological aspect of the transition to a new media platform, its economic aspects, as well as the transformation of the media system, competition between traditional and online publications, and the redistribution of

information flows and audience attention. The Internet was most often viewed as a means of democratizing public institutions, and an instrument for the implementation and protection of human rights and freedoms. Only a few authors considered that further development of the Internet could turn in a different direction and potentially become a "space of control" instead of a "space of freedom".

When considering the architecture of the Internet and the principles of its regulation, copyright occupies a special place, since it often becomes the main reason for addressing the problem of tightening cyberspace regulation. The very architecture of the network causes difficulties in controlling the exchange of content, and legal illiteracy. The associated ignorance of copyright law demonstrated by the vast amount of users has led to interested groups insisting on considering these issues only in the context of protecting copyrighted works, while overlooking other important aspects. At the same time, regulatory measures jeopardize precisely those areas related to open content and the public domain.

There are still serious contradictions between the very nature of the Internet, its technological capabilities and the rules formulated in the pre-digital era. Consideration of these contradictions in the context of the rights and various aspects of human freedom in the information society has given rise to a group of concepts related to the further development of cyberspace. However, most of them describe only certain aspects of the problem and are focused either on related issues such as the development of the information society, the public sphere, the media system, or, on the contrary, narrow legal topics. At the same time, the issues of freedom of the Internet and its regulation are especially relevant in connection with the latest legislative activities and initiatives both in Russia (the sovereign Internet) and in the European Union (Directive on Copyright in the Digital Single Market 2016/0280 [1]).

Literature review

The first works devoted to the Internet belonged primarily to the field of informatics. However, activists and media theorists attempted to outline the conceptual essence of the World Wide Web at the beginning of its development. In 1964 Marshall McLuhan described a global network, in many ways similar in nature to our central nervous system [2].

In the late 20th century many researchers pinned great hopes on the Internet, assuming that it would significantly transform social institutions, the worldview of social groups and would result in making the world and people completely different. Manuel Castells wrote in "The Internet Galaxy" that while technology does not guarantee freedom, the Internet is in fact a powerful tool for both the exercise of personal freedom and the freedom of social groups [3].

A similar point of view was held by the creators and pioneers of cyberspace who imagined it free from any kind of control as proclaimed in "A Declaration of the Independence of Cyberspace" [4]. Its author, John Perry Barlow, one of the

founders of the Electronic Frontiers Foundation (a non-profit organization), declared the independence of the Internet primarily from government control.

Nevertheless, even at this time, there were academics who presented a radically opposing point of view on the future of the Internet. As early as 1999, Harvard Law Professor Lawrence Lessig published his book "Code and Other laws of Cyberspace" [5]. Lessig pointed out that the Declaration of Independence was inaccurate in its core: "The claim for cyberspace was not just that government would not regulate cyberspace – it was that government could not regulate cyberspace" [6]. So according to this point of view "Cyberspace was, by nature, unavoidably free. Governments could threaten, but behavior could not be controlled; laws could be passed, but they would have no real effect" [6].

However, this key premise is false. The sense that freedom lies at the very foundations of the Internet environment was formed among researchers (or people with an academic background) primarily because of its architecture. This corresponded to ideas about cyberspace shared among a small group of "pioneers" – developers and activists who created and mastered the first websites and services [5].

As the number of Internet users began to increase, the digital environment began to attract more and more attention, first from business and then from the state. For example, the SORM-2 system, installed in Russia in 1999, provided government security services with the opportunity to access information transmitted by Russian Internet providers. Its introduction became a prerequisite for the emergence of a number of studies related to the control and freedom of the digital network. The results showed that the introduction of this system led to the withdrawal from the market of smaller companies that could not afford the installation of the requisite equipment [7]. Thus, these measures served not only as a means to increase political control over providers, but also as an instrument for increasing concentration of the provision of Internet access services in the interests of large operators, the most important of which is the state-owned "Rostelecom".

Among other significant works on the topic published at the dawn of the digital era, the Russian researcher M. Kasenova [8] highlighted the papers of J. Reidenberg [9] on the emerging contradictions in the definition of jurisdiction on the Internet, and M. Froomkin [10] and J. Zittrain [11] on the problems of cyberspace regulatory mechanisms.

A significant number of articles on the topic of control of the Runet is devoted to discussing the results of Roskomnadzor (Federal Service for Supervision of Communications, Information Technology and Mass Media) initiatives and performance. L. Sivets analyzes the impact of Roskomnadzor's interaction with the owners of the Internet infrastructure on the freedom of speech [12]. A series of publications published by The Berkman Center for Internet & Society are devoted to the development of Internet regulation in Russia. One article written by Andrey Tselikov describes and analyses the history of the development of state control over the Runet in the first 20 years of its existence

[13]. In other articles, regulation is closely linked to the concept of censorship and attempts by the state to ensure control over public discussion in the online environment [14]. Some studies from this group are devoted to the issues of piracy in Russia [15]. Piracy, fears for the safety of children, fear of foreign influence on the political agenda, reinforced by the "lessons" of the "Arab revolutions", have become key reasons for tightening the regulations.

Another area of research is associated with the "shadow" Internet, or "darknet". This is an environment where the law can be ignored and is often used for prohibited activities. As regulation becomes tighter, the darknet is taking on new functions and attracting a wider audience interested in, for example, keeping private correspondence secret. A number of articles on this matter were published in the "New Media and Society" in 2016–2017 [16]. The problem is also considered in a number of the studies by non-profit organizations dealing with Internet freedom issues [17, 18].

There are other points of view on the issue of freedom in the context of media and communication in general. K. Karppinen, for example, points out: "Especially in political debates on the media, but also in research, the status of freedom as a foundational ideal is often simply taken for granted, which leaves questions of normative assumptions unexamined… Despite the recognition of the decidedly non-ideal circumstances surrounding the contemporary media landscape, the debates tend to be couched in ideal frameworks of the free marketplace of ideas, the public sphere, or some other established model or metaphor of what communicative freedom would mean under idealized, hypothetical conditions" [19]. In practice, at the level of national jurisdictions, regulation occurs at the initiative of the most influential national actors depending on the specifics of the political and economic system. These can be the security services, government, copyright holders, state-owned companies, and publishers.

A separate block of studies is also devoted to the issues of Internet freedom in different countries of the world, including Africa and China. Articles by African academics in particular offer a balanced approach which takes into account the need to confront crime [20]. The perspective of Chinese researchers on Internet regulation in China differs significantly from the Western perspective. "This framework focuses on political control and tends to reduce China's policies to the attempts by an authoritarian state to elevate governments and intergovernmental organizations to be the only legitimate governors of global cyberspace. As it traces the evolution of China's relationship with the global Internet in the past three decades, the study demonstrates that China's stance is more complex than the prevalent framework allows and that it is both built upon and different from the US-centric, market-oriented Internet governance scheme" [21]. In practice, this approach is not only reactionary, but also project-based, as the introduction of a social rating shows. It is obvious that at the very outset the designation of the vast Chinese market as a separate ecosystem allowed the formation of a unique and independent industry. However, neither Russia nor any

individual country in Europe, South America or Asia has yet been able to repeat this experience, not even India, despite its huge market.

In this context, the approach to confronting different concepts of the Internet as different political and economic systems is also interesting: "cyber war is usually understood as a conflict between the «internet freedom» agenda <...> and the cause of «information sovereignty», promoted by governments such as that of China. In reality, it is not a war to defend freedom of expression online, but rather, «a competition among different political economies of the information society»" [22].

Many different approaches and research directions related to the development of ideas about the nature of the network and the possibilities of its regulation can be defined. This also concerns issues of human freedom which, on the one hand, received new tools for implementation, and on the other hand, face new threats.

Values and the nature of regulation

The role of code in the control of the cyberspace was formulated for the first time in the book by L. Lessig: "The single most significant change in the politics of cyberspace is the coming of age of this simple idea: The code is law. The architectures of cyberspace are as important as the law in defining and defeating the liberties of the Net. Activists concerned with defending liberty, privacy or access must watch the code coming from the Valley – call it West Coast Code – as much as the code coming from Congress – call it East Coast Code" [5].

In cyberspace, code is similar to the laws of physics in the real world, since the functions of Internet services and attaining certain freedoms directly depend on the architecture. In *Code 2.0*, Lessig describes the four main tools for regulating the Internet: law, norms, market, and architecture – the code. The preference for a particular tool usually depends on its potential effectiveness. In the real world, influencing the "code" – the architecture of space – is quite difficult, although such examples exist. Within the Internet environment, everything is much simpler, but it is the modification of the code that is often the most effective tool of Internet regulation.

From Lessig's point of view, the foundations of cyberspace, just like the constitution, must be built, they do not arise by themselves: "Foundations get laid, they don't magically appear. …Thus, as our framers learned, and as the Russians saw, we have every reason to believe that cyberspace, left to itself, will not fulfill the promise of freedom. Left to itself, cyberspace will become a perfect tool of control" [6].

Lessig singled out the following key issues for discussion: intellectual property, privacy and freedom of speech. In his opinion, based on these values we decide the principles pursuant to which the cyberspace should function [6]. As an example of values determining the design and functioning of cyberspace, Lessig

cites the difference in Internet regulation at the University of Chicago and Harvard: "In the former, a computer is enough to access the network. The Internet does not require authorization and the ports are open to everyone. At Harvard University, only verified and authorized users can access the network. Accordingly, in the case of Chicago it is almost impossible to track the activity of a specific person, while at Harvard, all actions are recorded and can be easily established in relation to any user. These two networks differ in at least two important ways. First and most obviously, they differ in the values they embrace. That difference is by design. At the University of Chicago, First Amendment values determined network design; different values determined Harvard's design" [6].

An important place in the new networked world is occupied primarily by issues of copyright which plays a key role for any manipulations with the digital content on the Internet. This raises the question of what is really paramount for society and the balance of interests between authors and users.

Intellectual property is the backbone of the digital economy. However, many researchers note that the principles of the industrial era are often inapplicable in the context of the information society. In particular, James Boyle draws attention to the fact that when discussing internet regulation the criterion of efficiency should also be taken into account. Expensive and limited access to information leads to a less effective market, academic community and computer industry [23]. Today not only academics, but also activists and representatives of NGO in Russian and the world share similar beliefs. Examples of these are the Webpublishers Association, one of founders is Maxim Moshkov, the creator of the Moshkov library, representatives of Wikimedia, researchers and activists. Webpublisher's research program and publications raise questions about a new model of copyright regulation based on the concept of the common good which form the position of progressive reforms in the field of copyright. However, even the noospheric normative media theory formed at the Department of New Media and Theory Communication of the Faculty of Journalism of Moscow State University touches only on a minor part of the problems discussed in this article.

Often it is not the content creators themselves or the nation-states that derive real benefit from the current system, but companies and corporations which have gained control over huge amounts of intellectual property: "The true irony comes when we find that large companies can use the idea of the independent entrepreneurial creator to justify intellectual property rights so expansive that they make it much harder for future independent creators actually to create. The expansion of intellectual property inhibits the very process on which the expansionists premise their arguments" [23].

Approaches to copyright protection regimes provide another example of the role of values in the regulation of human rights and freedoms. As Peter Baldwin [24] noted, there are two main approaches to copyright. These are the European and Anglo-American approaches each based on different conceptual foundations.

The French system goes back to human rights – the concept of inalienable moral rights appeared in France. In the United States a conceptually different production approach is being implemented. The author is primarily an entrepreneur who has the right to sell his works, including giving up his name. At the same time, according to Baldwin, in the European system, a work is "born" as the property of its creator (i.e. it is a "human right"). In the Anglo-American concept it is initially public domain, but the author is endowed with the right to benefit from it for some given period of time (conditionally, right of use or "copyright"). In matters of Internet regulation, these conceptual frameworks are also critically important since they determine the degree of freedom of handling copyright content and the balance of interests in the system.

The principles of regulating the Internet environment are based not only on political regimes, but also on the values shared by society. Therefore, a number of factors need to be taken into account when analyzing this issue. This, in particular, is indicated by the results of the study by Jaclyn Kerr: "While policies regulating or restricting online freedoms of speech, media, access to information, or association often parallel their "offline" equivalents, such "online-offline policy-linkage" is only part of the picture. Even among non- democratic regimes with similar levels of Internet penetration, we see fairly dramatic variation in how these technologies are regulated" [25].

The Internet and new aspects of freedom

The European Convention on Human Rights consists of 18 articles which describe 12 key rights and freedoms – in fact, the basic values that Western civilization is now guided by [26]. These include several articles directly related to the understanding of freedom on the Internet: a right to respect for one's private and family life, home and correspondence; freedom of thought, conscience and religion; freedom of expression; freedom of assembly and association.

Regulation of the Internet environment often poses a potential threat to these freedoms. It also raises questions about the ethics of certain control measures taken by the state. For example, from the point of view of the European Court of Human Rights the SORM system in Russia is a violation of the convention [27], and hence of human freedoms.

The ethical dilemma associated with the question of whether the use of surveillance devices is legitimate, if they do not in any way affect the lives of innocent people takes on a new appearance when applied to the Internet space. Lessig gives the example of a computer worm that aims to track a specific set of information on the hard drive of a personal device. "Is this an unconstitutional worm? This is a hard question that at first seems to have an easy answer. The worm is engaging in a government-initiated search of citizens' disks. There is no reasonable suspicion (as the law ordinarily requires) that the disk holds the document for which the government is searching. It is a generalized,

suspicionless search of private spaces by the government. <…> And perhaps more importantly, unlike the general search, the worm learns little and leaves no damage after it's finished: The code can't read private letters; it doesn't break down doors; it doesn't interfere with ordinary life. And the innocent have nothing to fear" [6].

How far is society willing to go in extending such secure control? This begs the question of whether the state can always be perceived as an impersonal agent of order, or, under the guise of the state, are we dealing with specific strategies of influential actors. The pandemic in 2020 raised these questions with renewed vigor and in a new way, while reducing the ability of society to resist the expansion of such control.

This reasoning brings back the thesis that the structure of cyberspace and the set of freedoms that people are willing to defend primarily on the value system. In the case of the Internet, politics and architecture are inextricably linked: "End-to-end is a paradigm for technology that embeds values. Which architecture we encourage is a choice about which policy we encourage. This is true even in the context in which the Internet is not a "place" – even where, that is, it is "just" a medium" [6].

The conditions for interaction with the virtual world are dictated not only by states, but also by specific services. Lessig describes an example of America Online: "This space is constituted by its code. You can resist this code – you can resist how you find it, just as you can resist cold weather by putting on a sweater. But you are not going to change how it is" [6]. The service determines the ability of a person to show or hide his identity. It creates opportunities for communication in a collective space or makes it impossible; it creates and implements surveillance tools, and obliges you to provide the data it needs. It is also the same with the other platforms – for example, Facebook, WeChat, VK or even Google. However, this observation cannot be considered an axima. Recent years have shown that companies are forced to respond to changes in legislation in each jurisdiction. It is another matter that the specific mechanism for their implementation often leads to a discrepancy between the result and the legislator's intention.

As mentioned above Intellectual property issues assume a particular importance in the context of the issues described: "Barriers within cyberspace – separate chat rooms, intranet gateways, digital envelopes, and other systems to limit access–resemble the effects of national borders, physical boundaries, and distance. Programming determines which people can access which digital objects and which digital objects can interact with other digital objects" [6]. This is why all new laws aimed at regulating the network often start with defining and drawing the boundaries between the different types of platforms and how they are used, labeling them as organizers of mass and private communication, or as broadcasters as per the 2019 European Copyright Directive – and applying new norms to them.

Another important aspect is the potential inability to circumvent the laws that are established by the code itself: "A locked door is not a command "do not enter" backed up with the threat of punishment by the state. A locked door is a physical constraint on the liberty of someone to enter some space" [6].

Other ethical issues raised by recent Internet legislation are also interesting. At a meeting of members of The Presidential Council for Civil Society and Human Rights in connection with the adoption of the "law against fakes", one expert expressed the opinion that a person always has had the right to lie. Lying can be considered a violation of ethical norms, and evoke public condemnation, but in general, from the point of view of legislation, a person always has the opportunity (and, therefore, the right) to lie. This may, for example, be in the form of interpreting circumstances to his/her favor or defending his/her position within the framework of an adversarial legal process (not to mention the human right not to testify against himself and his close relatives). Control over the Internet space, the proliferation of tracking and recognition systems can lead such a right being removed. It should be borne in mind that these changes are also a constraint upon freedom which was previously taken for granted, since they lead to the maximum compression of the space of privacy and the secrecy of correspondence. Although, perhaps, it is correct to speak not about the inability to lie, but about replacing the living communicative space with something similar to the media system limited by licensing laws, etc.

The Internet space exists according to completely different laws, since it is not conditioned by the material world. "Both "on the Internet" and "in cyberspace," technology constitutes the environment of the space, and it will give us a much wider range of control over how interactions work in that space than in real space. Problems can be programmed or "coded" into the story, and they can be "coded" away" [6]. At the same time, laws lean not only on punishment, but also on the general recognition that they are reasonable and meaningful. Otherwise, they stop working, even if it is formally possible to "serve the decencies". The issues described and the nature of cyberspace offer a new look at the issue of freedom of virtual worlds, in which their creator, for some reason, must lose all power over what is happening and adapt to the requests of local governments.

Conclusion

Studying the evolution of views on freedom on the Internet shows how the very concept of cyberspace has been transformed over several decades. If it all started with the assertion that the Internet will change the world and make it more free and democratic, then over time the discourse has shifted to questions about the principles of network regulation. A key place in the academic discussion has been occupied by the research of lawyers devoted to analyzing the norms and law enforcement practice, as well as the impact of national regulations and technological constraints which are being introduced by states around the world.

The development of ideas about how the Internet environment should be regulated (especially in Russia) is hampered by scarce attention to values as a key side of the issue. The discussion is mainly reduced to the fight against censorship, interference in privacy and the protection of personal data. At the same time, the broader context is ignored – issues of freedom and human rights in the Internet environment, discussion of what is really important for our society – security or freedom, trust in the state or the services that people use. Such examples as the blocking of Telegram in Russia have clearly demonstrated that in some cases users are much more willing to entrust their personal data and privacy to a third party (including foreign companies) than to their national state institutions. Such are inextricably linked with national regulation, as well as legislation, for example, on administrative violations and criminal offenses, law enforcement agencies and special services, Primarily because in the first case they essentially ensure immunity from prosecution, and in the second they become easy prey.

By being born in a certain country and obtaining its citizenship, a person becomes limited in the choice of norms and laws that he or she is forced to follow under the threat of persecution. The Internet gives people a choice in the services they want to use and are willing to trust. However, states are now trying to limit this freedom as much as possible, declaring their right to regulate the Internet space with the laws of a particular country. From a philosophical point of view, the question of how adequate and justified such an approach may be remains controversial. However, practice, including law enforcement, indicates that the state is not ready to leave this freedom of choice to its citizens.

References

[1] *Proposal for a Directive 2014/27/EU of the European Parliament and of the Council on copyright in the Digital Single Market.* Retrieved May 3, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0593

[2] McLuhan, M. (1994). *Understanding Media: The Extensions of Man.* New York: MIT Press.

[3] Castells, M. (2003). *The Internet Galaxy: Reflections on the Internet, Business, and Society.* 1st edition. Oxford: Oxford University Press.

[4] *A Declaration of the Independence of Cyberspace.* Retrieved May 3, 2020, from https://www.eff.org/cyberspace-independence

[5] Lessig, L. (1999*). Code and Other Laws of Cyberspace.* New York: Basic Books.

[6] Lessig, L. (2006). *Code version 2.0.* New York: Basic Books.

[7] Alexander, M. (2004). The Internet and Democratization: The Development of Russian Internet Policy. *Demokratizatsiya The Journal of Post-Soviet Democratization, 12*(4), 607–627. (In Russ.)

[8] *Evolution of the concepts of cross-border Internet use in foreign legal doctrine.* Retrieved May 3, 2020, from http://inter-legal.ru/evolyutsiya-kontseptsij-transgranichnogo-ispolzova-niya-interneta-v-zarubezhnoj-pravovoj-doktrine (In Russ.)

[9] Reidenberg, J. (2005) Technology and Internet Jurisdiction. *University of Pennsylvania Law Review,* (153), 1951–1974.

[10] Froomkin, A. (2005). International and National Regulation of the Internet. In *The Round Table Expert Group on Telecommunications Laws: Conference Papers.*

[11] Zittrain, J. (2006). The Generative Internet. *Harvard Law Review.*

[12]   Sivetc, L. (2019). State regulation of online speech in Russia: the role of internet infrastructure owners. *International Journal of Law and Information Technology, 1*(27), 28–49.

[13]   Tselikov, *A*. (2014). The Tightening Web of Russian Internet Regulation. In *Berkman Center Research Publication,* 2014–2015.

[14]   Etling, B.*,* Faris, R., Palfrey, J., Gasser, U., Kelly, J., & Alexanyan, K. (2010). Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization (2010–2011). *Berkman Center for Internet & Society of Harvard University.*

[15]   Mickiewicz, E. (2015). Piracy, policy, and Russia's emerging media market. *The Harvard International Journal of Press/Politics, 2*, 30–51.

[16]   Gehl, R. (2016). Power/freedom on the Dark Web: a digital ethnography of the Dark Web social network. *New Media & Society, 18*(7), 1219–1235.

[17]   *Human Rights Watch. Race to the bottom: corporate complicity in Chinese Internet Censorship.* Retrieved May 3, 2020, from https://www.hrw.org/reports/2006/china0806/china0806web.pdf

[18]   *Freedom on the Net 2015: privatizing censorship, eroding privacy.* Retrieved May 3, 2020, from https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf

[19]   Karppinen, K. (2019). Freedom Without Idealization: Non-Ideal Approaches to Freedom of Communication. *Communication Theory, 1*(29), 66–85.

[20]   Turianskyi, Y. (2018). Balancing Cyber Security and Internet Freedom in Africa. *Africa Portal.*

[21]   Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication, 9*(3), 304–324.

[22]   Powers, S., & Jablonski, M. (2016). The real cyber war: The political economy of internet freedom. *New Media & Society, 18*(6), 1054–1056.

[23]   Boyle, J. (1997). *Shamans, software, and spleens: law and the construction of the information society*. Harvard University Press.

[24]   Baldwin, P. (2015). *The copyright wars: three centuries of trans-Atlantic battle*. Princeton, New Jersey: Princeton University Press.

[25]   Kerr, J. (2014). The Digital Dictator's Dilemma: Internet Regulation and Political Control in Non-Democratic States. *Social Science Seminar.*

[26]   *European Convention on Human Right.* Retrieved May 3, 2020, from https://www.echr.coe.int/Documents/Convention_ENG.pdf.

[27]   *Review of the practice of the Supreme Court of the Russian Federation 3 (2016): decisions of the ECHR*. Retrieved May 3, 2020, from http://europeancourt.ru/tag/roman-zaxarov-protiv-rossii. (In Russ.).

Bio notes:

Ivan I. Zassoursky, PhD in Philology, Head of the Department of New Media and Communication Theory, Faculty of Journalism, Lomonosov Moscow State University. ORCID: 0000-0002-2524-6168; e-mail: zassoursky@gmail.com

Nataliia D. Trishchenko, PhD in Philology, Senior Researcher, the Department of New Media and Communication Theory, Faculty of Journalism, Lomonosov Moscow State University. ORCID: 0000-0002-6834-6206; e-mail: trishchenko.nataliia@yandex.ru

Сведения об авторах:

Засурский Иван Иванович, кандидат филологических наук, заведующий кафедрой новых медиа и теории коммуникации факультета журналистики МГУ имени М.В. Ломоносова. ORCID: 0000-0002-2524-6168; e-mail: zassoursky@gmail.com

Трищенко Наталия Дмитриевна, кандидат филологических наук, старший научный сотрудник кафедры новых медиа и теории коммуникации факультета журналистики МГУ имени М.В. Ломоносова. ORCID: 0000-0002-6834-6206; e-mail: trishchenko.nataliia@yandex.ru