

National Sovereignty: Socio-Political Transformation in Context of Modern Cyber Realities

Mamychev Alexey Yurievich¹, Zolochevskaya Elena Yurievna², Miroshnichenko Olga Igorevna³, Yevtushenko Sergey Aleksandrovich⁴ & Kerimov Oleg Yuryevich⁴

¹ Department of Legal Foundations of Administration, Moscow State Institute of International Relations, Moscow, Russia

² Russian Presidential Academy of National Economy and Public Administration, the Southern Russian Institute of Management – Branch, Russia

³ Department of Theory and History of State and Law, Far Eastern Federal University, Vladivostok, Russia

⁴ Department of Political Science and Ethnopolitics, Russian Presidential Academy of National Economy and Public Administration, the Southern Russian Institute of Management – Branch, Russia

Correspondence: Mamychev Alexey Yurievich, Department of Legal Foundations of Administration of Moscow State Institute of International Relations, Moscow, Russia. E-mail: mamychev@yandex.ru

Received: May 25, 2019

Accepted: July 4, 2019

Online Published: July 10, 2019

doi:10.5539/jpl.v12n3p11

URL: <https://doi.org/10.5539/jpl.v12n3p11>

The study was carried out with the financial support of the Russian Foundation for Basic Research in the framework of research project No. 18-29-16129

Abstract

The key idea of the study is the question of the relationship between such categories as “national sovereignty” and “cyberspace”. The authors consider that the current theory of law and positive legal regulation at the present stage do not offer reasonable options for interaction and coexistence of these concepts.

In the conditions of the dramatic changes in the existing realities over the past 30 years, the question arises of the differentiation of legal regulation, which is still more intended to the social relations that existed in the 20th century. Today technical progress is significantly ahead of social, in particular, legal regulation, which, in turn, is seriously tied to the state or, as any law student confirms, “territorial organization of power in a society with sovereignty...”. And here the main question arises about the reasonableness of the above formulation. Is it suitable for existing realities? Or is it itself an obstacle to legalization? The article analyzes various approaches to the legal settlement of relations in cyberspace, as well as offers two options for supranational regulation of these legal relations - through the development and establishment of an extraterritorial international body that will have not only the ability to control public relations within cyberspace, but also special instruments of coercion to influence the citizens of any state, either through the creation of a global system of international acts that will regulate most of the existing questions about the interaction of persons in cyberspace and included a clear mechanism to respond quickly to the emergence of new relations in this sphere.

The authors also consider that the inability at theoretical level to conceptualize the relationship between these categories could lead to the discrediting of such notions as “national state” and “national sovereignty” in the future.

Keywords: national sovereignty, cyberspace, national jurisdiction, cyber net

1. Introduction

Modern innovation and technological achievements of modern society, the development of digital technologies such as virtual and augmented reality, the spread of network communities, passing any state-legal boundaries, ethnopolitical markers, etc., problematize both the concept of the state and its sovereign qualities. Even 20-30 years ago, a person who doubted the power of the Gobbs Leviathan (state) or expressed his opinion about “robotization through globalization” seemed like an eccentric and a dreamer.

Today the idea of a “global village”¹ not only doesn't seem as utopia, but often scares its reality. At the level of modern theory politicians seriously reflect on virtual technologies and digital subjects of public-power interaction.

Within the framework of legal science, the idea of a cyber legal system is firmly shaped, which does not exist within any territorial framework, but nevertheless has all the features of this theoretical category. But the most interesting (or frightening, depending on the subject and context of consideration) is that the actors of the new space, the so-called cyberspace, are less concerned about the calculations of scientists and theorists. Giants like Amazon, Facebook, etc. in fact, prove their worth by giving scientists only analytics of their own activities.

Thus, it is simply unreasonable to deny the cardinal changes of the existing realities over the past 30 years. This raises the question of the differentiation of legal regulation, which is still designed to a greater degree on the social relations that existed in the 20th century. Today, technical progress is significantly ahead of the socio-political, in particular, legal regulation, which, in turn, is seriously tied to the state – “the territorial organization of power in a society that has sovereignty ...”.

And there is a whole series of questions, which is, undoubtedly, linked and defined the problems of this work: as the wording is reasonable? Is it appropriate to describe the unfolding realities? Is this a scientific metaphor or an adequate concept to describe a political reality, which can also be used for legal reasoning?

Active using of modern technologies in the citizens' life in most countries of the world community becomes necessity. But what to do with the main countries duty - protection of the rights and legitimate interests of citizens, which is very complicated in the modern “cyber realities”?

In particular, in the attempts of states to protect the interests of their citizens in a space that does not have geographic boundaries, the problem arises of correlating such categories as national sovereignty and cyberspace.

We consider that the main issue in this context is the modernization of the classical concept of national sovereignty. If today we do not revise the main theoretical categories, we can receive risk of coming to the realization of the principle proclaimed by the Declaration of Independence of Cyberspace: “cyberspace is the so-called terra nullius, to which historically created social regulations and laws are irrelevant and within which they will be recreated again”².

2. Main Part

The theory of sovereignty and its transformation in the XXI century. Obviously, before discussing the transformation of the classical theory of sovereign qualities of the state, it is necessary to distinguish between the two concepts under discussion - sovereignty and hyperspace, highlighting not only their specific characteristics, but also possible common features.

We use for example the classical definition of “sovereignty” which advantageously is treated as a technical category³ or attributive political and legal quality of the state⁴. In this aspect sovereignty is an integral political and legal quality of the state, a necessary constitutional characteristic reflecting state-territorial integrity, supremacy and legal unity, as well as the ability of the state to be an independent representative of society in the international legal arena, and independently implement fundamental functions, priorities and directions of the legal policy of the latter. In other words, a sovereign state in international law is considered to be such state whose jurisdiction extends over its entire geographical territory and does not depend on the jurisdiction of another state⁵.

Processes of reviewing of “sovereignty” category are regarded today as a natural and rather obvious outcome of the formation of a new stage of internationalization - the global world order⁶.

Moreover the new presentation of format of this category is connected in practical terms with the formation of the global world political order, its standards, parameters and mode of functioning, rules and support systems, and in a

¹ Kaijuka Ezron, (2018). *The world of Innovations and Cyber Law*. URL. https://www.academia.edu/37992759/the_world_of_innovations_and_cyberlaw.docx

² Barlow, J. P., (1996). *Declaration of Independence of Cyberspace*.

³ Kukushkina, S.M., (2011). Gosudarstvennyj suverenitet v sovremennom mire: actual'nye problem (National Sovereignty in the Modern World: Actual Problems), *Probely v rossijskom zakonodatel'stve*. № 3. pp. 84-86.

⁴ Mamychev A.Y., (2018). *Gosudarstvennaia vlast' v socio-kul'turnoj organizacii sovremennogo obschestva: teoreticheskoe-metodologicheskie aspekty politico-pravovoj transformacii* (State power of the sociocultural organization of modern society: theoretical and methodological aspects of political and legal transformation). Moscow: RIOR, INFRA-M.

⁵ Marchenko M.N., (2003). Gosudarstvennyj suverenitet: problemy opredeleniia poniatii i sodержannia (National sovereignty: problems of defining the concept and content). *Pravovedenie*. No. 1. pp. 186-197.

⁶ Fukuyama F., (2007). *Sil'noe gosudarstvo: upravlenie i mirovoj poriadok v 21 veke* (A Strong State: Governance and the world order in the XXI century). Moscow: Hranitel.

theoretical sense - with the formulation of non-state (international) axioms and values, a new planetary cosmopolitan worldview.

It's clear and understandable, because the main emphasis in political rhetoric and scientific research is not on the objective global trends, socio-cultural dialogue and exchange, but rather on the process of formation of a new *post sovereign world order*.

Modern project of attaining post sovereignty for legal entities of the state examines and analyzes the state power not as before - in terms of national and cultural uniqueness (proximity or remoteness of the political, social, spiritual, legal, economic and other development), and through the prism of inclusion of states in the formed order, compliance with its standards and legitimation of a political regime by the international community. In this globalist discourse another conceptual series, a different logic for the consideration of problems are used. Thus, the problem of security is transferred from the sovereign territories and viewed in terms of an international point of view (non-territorial, planetary, universal).

The legality and legitimacy of extraordinary situations and emergency regimes is justified not through ensuring integrity, unity, stability of the sovereign state, but through international sanctioning, i.e. recognition of these actions as necessary for the preservation, promotion of a global order and the corresponding ideology.

In general, the processes of development of the global political communication don't only "introduce" new actors of interaction, but also change the usual forms and technology of recognition and approval of public decision-making. So, today in the global political process, national system of state power serves only one of the actors on par with multinational corporations, non-governmental organizations, the international community and so on. And the solution of global problems, according to a just conclusion Ulrich Beck, "opens new, extra-democratic, extra-state sources of legitimacy justify itself: the vote is replaced approval"⁷. In this changing format of political cooperation at the global level national forms of legalization and legitimization of public activity are completely ignored, treated as ineffective, inadequate, not meeting the new principles, rules and objectives of the global political process.

Becoming of post sovereign order led to a diffusion of derived from the government's sovereignty category "legitimate and legal violence", "whereas he discourse of human rights, along with the military interventions and legal actions, - noticed the modern researchers M. Hart and A. Negri, - was part of a gradual movement to delegitimize the violence wielded by nation-states even within their own national territory"⁸. In this situation the disappearance of the monopoly (sovereign) right of the state to legal and legitimate enforcement introduces disturbing issues: "If the violence wielded by the nation-state is no longer considered legitimate a priori, based on its own legal structures, then how is violence legitimated today? Is all violence equally legitimate? Do Bin Laden and al-Qaeda, for example, have the same legitimacy that the United States military has to exercise violence? Is the violence of Palestinian groups wielded against Israeli citizens just as legitimate as the violence of the Israeli military against Palestinian citizens?" So in the world order "where - continues the above-mentioned author - no violence can be legitimated, all violence can potentially be called terrorism... the contemporary definitions of terrorism are all variable and depend on who defines their central elements: legitimate government, human rights, and rules of war".

In line with the above, we should make a major theoretical and methodological note for subsequent analysis of processes of desovereignization: quite entrenched in contemporary research practice was the approval of the objectivity of the processes of globalization, or more specifically, the objectivity of the processes of global transformation of the state and law. One can only partially agree with this, since interstate cooperation seems to be natural in solving many global problems. However, this does not mean that the process of global unification of its national law, the withering away of the sovereign quality of public authorities has objective character.

National sovereignty vs hyperspace. Thus, national sovereignty is politico-territorial and legal field, which keeps it safe legal policy of a particular state, the organization of public relations in this state and allows limiting the impact of globalization on the relationship entered into by its citizens. Its role has significantly decreased with the development of information communications and technologies, which have created a separate space that is not subject to geographical differentiation.

⁷ Beck U., (2007). *Vlast' i ee opponenty v epohu globalizacii. Novaia vseмирno-politicheskaia ekonomia* (Power and its opponents in the epoch of globalization. New global political economy). Moscow: Progress-tradiciia.

⁸ Hradt M., Negri A., (2006). *Mnozhestvo: vojna i demokratiia v epohu imperii* (Set: war and democracy in the era of the empire). Moscow: Kul'turnaia revoliuciia.

The United States Supreme Court defines cyberspace as a unique medium - known to its users as “cyberspace” - located in no particular geographical location but available to anyone, anywhere in the world, with access to the internet. In turn, the International Organization for Standardization gives the following definition of cyberspace: complicated medium which results from the interaction of people, software and services on the Internet by means of technological devices and networks connected to it, which does not exist in any physical form⁹ .

In this way we can conclude that cyberspace is information fields, created on the basis of a general Internet, in which social relations of a legal nature appear, aren't defining any territorial boundaries.

In light of this, the question of the relationship between the categories cyberspace and national sovereignty in international law is relevant, because the scope of the first phenomenon, as well as the jurisdiction of a particular state, is traditionally determined its territory. Cyberspace is not material and is not subject to geographical scope, so that there is a problem to define a sphere of state jurisdiction on a specific amount of cyberspace. Moreover, the question arises about the very possibility of determining the jurisdictional borders of states in cyberspace.

Undoubtedly, cyberspace is the medium in which, social relations of a legal nature appear. However, in contrast to the legal relationships realized within the territorial jurisdiction, their cyber analogues are not subject of regulation of any specific state, causing a problem of protection of rights and interests of citizens, if they enter into relationships via cyber network.

So, in a case of *American Libraries Ass'n v. Pataki* the US Court concluded that the geographical scope may not be applicable to the Internet. He proclaimed that users of a particular Internet resource do not know and are not interested in his physical location. The court stated that the Internet protocols were designed to ignore rather than confirm geographic location. In fact, this legal opinion speaks of the uselessness of geographical boundaries in the Internet.

However, there is a categorically different point of view on “territoriality” and the required type of regulation of cyberspace, which is proclaimed and promoted, in particular, by such states as Russia and China. From the point of view of the designated approach, so-called codes of conduct should exist within each specific state, denoting specific country regulation principles of cyberspace. In other words, in this case, the cyber environment is not a sphere of free exchange of information between the actors, regardless of their nationality, citizenship and other characteristics, but rather a part of the national legal system that is quite clearly regulated by positive law.

In any case, it is obvious that at the present stage international law, proceeding mainly from the principle of territoriality, is not ready for a clear settlement of legal conflicts in which non -territorial organizations such as the Internet are involved¹⁰ .

World experience demonstrates quite a number of attempts to establish the boundaries of cyberspace by means of identification. The most predictable method of the principle of sovereignty in cyberspace is the attempt to identify information on the network and its relation to a particular state. For example, websites contain URL indicators of origin like “ru”, “nl”, but this does not contribute to the spread of the sovereignty of a state to relations that arise in connection with the interaction of a particular subject of law with such identified information. Due to the fact that access to specific information in cyberspace can be obtained by any person, regardless of his location, the policy of spreading the jurisdiction of a particular state to particular information in the network is meaningless¹¹ .

As the information in any case will be in the global access and relationships that arise regarding this information can't be settled within the jurisdiction of one state, at least due to the fact that in this case the subject of such relationship can't be a citizen of a country whose information he used.

That is why the definition of jurisdiction on the location of information on the server is not correct. For example, in the case of *Steven Rambam v. JDO*, the US court found the inadequacy of the criteria for finding a server to establish jurisdiction¹² .

⁹ Menthe Darrel, (1998). *Jurisdiction In Cyberspace: A Theory of International Spaces* 4 Mich.Tel.Tech.L.Rev.3 April 23. URL: <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1163&context=mttlr>

¹⁰ Kristen E. *The Cyber-Law of Nations*. California; Los Angeles (UCLA) URL: <https://georgetownlawjournal.org/articles/63/cyber-law-of-nations/pdf>

¹¹ *American Libraries Ass'n v. Pataki* 1997. *U.S. District Court for the Southern District of New York*. URL: <https://law.justia.com/cases/federal/district-courts/FSupp/969/160/1808497/>

¹² Anselmo Erin, (2006). *Kiberprostranstvo v mezhdunarodnom zakonodatel'stve: oprovergaet li razvitie interneta princip territorial'nosti v mezhdunarodnom prave?* (Cyberspace in international law: Does the development of the Internet refute the principle of territoriality in international law?) *Economic strategies*. № 2. pp. 24-31.

The transfer of the content of one site to the address of another, which is manifested in the presence of cross-references, makes the policy of identifying of Internet resources even more conditional, and is an integral part of the global network. So this characteristic of cyberspace is due to specific of the Internet, and so makes the obvious ineffectiveness of the concept of territoriality and geographical jurisdiction in international law, as in the information space connections with the physical location is almost lost¹³.

In the context under discussion it should be concluded that there is a need to develop principles of international law that otherwise differentiate the legal regime of cyberspace, and thus solve the problem of possible state-cybernetic conflicts. The problem of exercising national sovereignty and jurisdiction in cyberspace can't be settled independently in any state, based only on existing national legislation. The solution to this problem is possible only by the adoption of the relevant international convention.

Thus, the introduction of the Internet and Information and Communication Technologies in the field of international legal regulation is necessary, since modern technologies supplant the concept of geographic territoriality. However, such innovations may jeopardize the fundamental principles of traditional international law.

We consider that international law should adapt its dogmas to non-territorial informational formations, in particular, through an adequate interpretation of the category of "national sovereignty". Only in this case the concept of national sovereignty will be relevant in the context of informational globalization.

David Post and David Johnson also follow this position and saying that many of the jurisdictional and other significant problems arising in the field of comprehensive communication technologies can be solved using one simple principle: the idea of cyberspace as a separate "place" for legal analysis by recognizing the legally significant boundary between cyberspace and the "real world". They believe that cyberspace cannot and should not be settled by those institutions of international law that carry out legal regulation in material territory.

Consequently, the impossibility of equating the territorial boundaries to virtual is apparent, as well as it's impossible to use traditional conception of sovereignty in cyberspace.

From a theoretical point of view the ideal model of regulation of social relations in the framework of cyberspace are the projects of virtual states created in cyberspace. For example, J. Ferguson and R. Mensbach speak that "Free Burmese Coalition" as one of these states. Geographically this state exists only in cyberspace and "offers its support, which is difficult to achieve a geographically"¹⁴. Therefore models of such states ideally can protect the rights of their "citizens", regardless of their geographical location.

Another example that we would like to point out is that in the theory of sovereignty is "embedded" the concept of national-cultural identity and social integrity. At the same time modern hyperspace within the structuration of online communities, groups, and so on use many of these traditional elements, fragmenting and adapting them to define the boundaries of the virtual community and identify¹⁵. In other words, the formed socio-cultural, political and legal mechanisms are used as virtual technologies of "social assemblage"¹⁶, delimitation occurs (definition of the boundaries of the virtual community, establishment of virtual markers, symbols, etc.) and identification (friend-or-foe identification, procedures of inclusion in the community, management of turnover, etc.)

Moreover, in the context of the structuration of online communities, there is also the establishment of standards, codes of conduct, ethical standards and authorities (assembly points in network interaction), etc. However, as the leading motivational bases of these "virtual assemblies" in modern hyperspace and the very active actors to a greater degree are not traditional ideological and semantic elements or an orientation toward value-normative unity. But forms of social, political, ethnic, and other self-actualization have free construction and change of the boundaries of social communities and the development of online communication.

This problem, of course, requires a separate research, but here it should be noted that there is an obvious increase in the deep-seated contradictions between associative, network (online) communities, global structures of

¹³ Jewish Defense Organization, Inc. v. Superior Court (Rambam), (1999). *Court of Appeal, Second District, Division 7, California* URL: <https://law.justia.com/cases/california/court-of-appeal/4th/72/1045.html>

¹⁴ Iskevich I.S., Kochetkova M.N. and Popov A.M., (2016). Aktual'nye problemy opredeleniya yurisdikcii pri rassledovanii prestuplenij v informacionnom prostranstve: mezhdunarodno-pravovoj aspekt (Actual problems of determining jurisdiction in investigating crimes in the information space: the international legal aspect). *Problemy pravoohraniitel'noj deiatel'nosti*. No. 4. pp. 54-59.

¹⁵ Brown K. and Kaya S., (2000). *The problems of International Finance Law And Electronic Commerce*. Sydney.

¹⁶ Johnson David R. and Post David G., (1996). Law and Borders—The Rise of Law in Cyberspace, *Stanford Law Review*. vol. 48, pp. 1367-1402.

hyperspace and off-network (offline, traditional) forms of sociocultural communication and political mobilization on which classical theory of sovereignty based.

The problem of the relationship between the categories of “national sovereignty” and “cyberspace” assumes an increasing importance since the unsettledness of this issue may entail serious international conflicts and international legal conflicts. We also consider that the inability at the theoretical level to conceptualize this ratio may lead to the discrediting of such notions as “national state” and “national sovereignty” in the future.

3. Conclusion

At present there is an urgent need, firstly, in the conceptualization and meaningful design of cyberspace as a sphere for the implementation of social relations, including the legal type. So, either we consider cyberspace, according to Barlow, a freely functioning and not involving the intervention of the state environment - this is the first, in our opinion, extremely unlikely option. In the case if we attempt to include cyberspace in the existing theoretical categorical and conceptual apparatus, the urgent need to change the existing legal tools, both the fundamental theoretical and the positive legal, becomes quite obvious.

In our opinion, within the framework of the second aspect of this problem, the most promising are two ways:

1) The attempt to design and create outside the territorial international body, which will not only have the ability to control social relations within the framework of cyberspace, but also by special levers of coercion for the impact on the citizens of any state. This option is the “ideal solution” of the posed problem, since in this situation the traditional concept of national sovereignty in international law will not lose its meaning.

Though we consider that the probability of its realization is low, since the creation of such a large-scale structure, having the ability to coercion and not falling within the jurisdiction of one or another state is extremely risky for the international community. An attempt to take such step was envisaged in the Budapest Convention on Cybercrime, prepared by the Council of Europe in 2001¹⁷. The Convention was signed by representatives of 30 countries in November, 2001. It created a transnational body operating in real time and having the ability to delete materials regardless of the physical location of the Internet resource. However, the provisions of the Convention and have not been realized¹⁸.

2) Creating a global system of international acts that would regulate the most of existing questions about the interaction of people in cyberspace and included a clear mechanism to respond quickly to the emergence of new relations in this sphere. Thus, the concept of sovereignty in international law would include not only a geographic territory, but also the scope of potential actions and opportunities that a particular state can perform, as an actor in cyberspace. An attempt to create such an agreement has taken Russian Federation in 2011. The concept of the Convention on ensuring international information security was a draft of a global international document covering all the key issues of countering threats from cyberspace in the broad Russian understanding.

However, this approach met with sharp resistance from the United States. US Deputy Secretary of State M. Pozner stated that the proposals “transforming the Internet from a space controlled by a multitude of people and interested parties into a system controlled by central governments” are unacceptable¹⁹. In other words, this option is also difficult to realize, because in the opinion of some of the world community, it can contradict basic principles of democracy²⁰.

It is necessary to revise and substantively correct both the theory of sovereign state itself and the analysis of modern digital technologies for transferring the “sovereign characteristics” of state power to the structuration and legal regulation of hyperspace by a number of states. It is obvious that the concept of national sovereignty cannot be applied to the formulated models of a virtual state, since we are not talking about real territory or the jurisdiction of a particular traditional state. However, based on the foregoing, it also follows the conclusion that the idea of a “super-legal” regulation of relations arising in cyberspace can in principle exclude the classical

¹⁷ Ferguson Y.I., (2000). Technology and the Transformation of Global Politics / Y.H. Ferguson, R.W. Mansbach. *Paper prepared for the 2000 Annual Meeting of International Studies Association*, Los Angeles, March

¹⁸ Mamychev Aleksey Yu., Okorokov Aleksandr V., Bespalova Tatyana V. and Sviridkina Elena V., (2018). Civilizational modeling of political and legal development of the society in the XXI century. *Amazonia Investiga*. Vol. 7. Núm. 15 (Julio-Agosto 2018). pp. 49-57.

¹⁹ Lo J., (2015). *Posle metoda: besporiadok i social'naia nauka* (After the method: disorder and social science). Moscow: Institut Gajdar.

²⁰ Convention on Cybercrime ETS N 185: Budapest. (2001). November 23. *GARANT Legal Reference System*. URL: <http://base.garant.ru/4089723/>; Sharifov M.Sh., (2009). Suverennaia vlast' v kiberprostranstve i v setevom prostranstve (Sovereign power in cyberspace and in network space). *Sovremennoe pravo*. № 6. pp. 40-44; Bedritsky A.V., (2012). Mezhdunarodnye dogovorennosti po kiberprostranstvu: vozmozhn li consensus? (International agreements on cyberspace: is consensus possible?). *Problemy nacional'noj strategii*. № 4 (13). pp. 119-136.

understanding of sovereignty in international law or form a new theoretical and practical model of sovereign hyper-sovereignty.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).