Acta Universitatis Wratislaviensis No 3888
PRAWO CCCXXVII Wrocław 2019

DOI: 10.19195/0524-4544.327.21

ANDREY A. SHCHERBOVICH
ORCID: 0000-0002-4312-4025
National Research University Higher School of Economics, Russia
ashcherbovich@hse.ru

Comparative analysis of legislation in the sphere of Internet governance in Central and Eastern Europe

Abstract: The article deals with a comparative analysis of provisions of national legislation and draft legislation initiatives of the nations of Central and Eastern Europe on regulation of the Internet. Special attention is paid to legislative measures infringing human rights of Internet users. Here we need to stress the importance of international law which could guarantee realization of the human rights of users, as well as integrity of the Internet. Finally, the article suggests the most important provisions of the international rules for these purposes.

Keywords: Internet governance, human rights, Central and Eastern Europe, Council of Europe, cybersecurity, restrictive measures.

Internet governance processes are developing now throughout the world. The examined region of Central and Eastern Europe is within the framework of regional organizations, namely the Council of Europe (CoE), Organization for Security and Cooperation in Europe (OSCE) and partly the European Union. That means national legislations of the considered countries must comply with the standards and regulations of the European regional organizations.

International public law regulates the relations between nation states. Some international public law instruments already deal with areas of relevance to Internet governance (e.g., telecommunications regulations, human rights conventions, international trade treaties).

A number of elements of international public law could be used for Internet governance, including treaties and conventions, customary law, soft law, and *ius*

cogens (compelling law — a peremptory norm). As Jovan Kurbalija states, apart from the ITU conventions, the only convention that deals directly with Internet-related issues is the CoE Convention on Cybercrime.[1]

Here we would like to outline priority issues on which national legislation regulating the Internet is concentrated. Most examples provided here show us that the human rights of internet users are not always guaranteed.

Cybersecurity issues

There is a convention of the European Council on the protection of individuals with regard to Automatic Processing of Personal Data.[2] Russian legislation on personal data does not comply with this convention. The main legal problem in this area is the location of personal data of Russian citizens.

Location of personal data of Russian citizens, introduced by amendments to the Federal Law "On Personal Data" (Law No. 242-FZ),[3] is contrary to the nature of the Internet as an international network. Despite the fact that, technically, this kind of location is possible, there are many questions concerning the realization of the constitutional rights and freedoms of citizens. In fact, the adoption of this law was an unprecedented measure that could affect the existence of the entire Internet in Russia.

Starting from September 1, 2015 Internet services that deal with Russian citizens' personal data, should enable the processing of such data using a database located in Russia. The document concerns first of all, online stores, social networking, ticket reservation services, hotels and other services. It comes as Russian companies, which store data abroad and for foreign organizations that deal with clients from Russia.

The law has caused quite a strong reaction in the online community and among Internet industry experts. Traditionally, what the authors of the document are accused of is that it is almost unrealizable, and in practice, in no way does it ensure the security of Russian citizens, but rather complicates their lives and hampers the development of the Internet in Russia.

The reason for the adoption of the law formulated by its authors is as follows. Many people are active on social networks, as well as buying goods and services

[1] See: J. Kurbalija, *An introduction to Internet Governance*, 7th ed., Geneva 2017, p. 126.

[2] See: Convention for the Protection of Individuals with Automatic Processing of Personal Data. It was concluded in Strasbourg on 28.01.1981 (ConsultantPlus Legal Reference System).

[3] Federal Law No. 242-FZ of July 21, 2014 "On Amendments to Certain Legislative Acts of the Russian Federation Regarding Specification of the Procedure for the Processing of Personal Data in Information and Telecommunication Networks" (as amended on December 31, 2014) (ConsultantPlus Legal Reference System).

via the Internet. A significant portion of these services could be placed abroad, mainly in the US and Europe. As a result, credit card information, passport details, correspondence, including e-mail, could be accumulated by intelligence services of the states concerned.

As stated by one of the developers of the law, First Deputy Chairman of the Duma Committee on Information Policy, Information Technology and Communications Vadim Dengin, the majority of Russians are opposed to the storage of their personal data abroad and wish to remain in the territory of Russia. Otherwise, such information as a result of hacking attacks on foreign intelligence services may fall into the hands of fraudsters.[4]

The Act regulates the duties of operators to ensure the recording, systematization, accumulation, storage, clarification (update, change), and retrieval of personal data of Russian Federation citizens in database information located on the territory of the Russian Federation, as well as an indication of information about the location of such databases.

The Federal Service for Supervision of Communications, Information Technology and Mass Media **(**Roskomnadzor) is entitled on the basis of an enforceable court decision to limit access to information processed in violation of the Russian Federation in the field of personal data legislation. The law defines the procedure for limiting access to information processed in violation of the Russian legislation in the field of personal data. For this purpose, there exists an automated information system "Register of violators of the law on personal data."

In Romania, the Parliament approved a law — initiated by the government — on network and information security (NIS). Transposing the EU NIS Directive into national legislation, the law establishes NIS-related obligations for operators of critical services (these operators will be determined by the national CERT and included in a classified national register), as well as for providers of digital services. The Ministry of Communications and Information Society is entrusted with the strategic coordination of NIS activities in terms of public policy and legislative initiatives, while CERT-RO becomes the authority competent at the national level for the security of networks and systems which ensure the provision of critical services or of digital services. The government is to adopt a national NIS strategy within six months after the law enters into force.[5]

---

[4] See: A. Filimonov, "'Delit′sâ nado!' ili Zaŝita personal′nyh dannyh rossiân ot inostrannyh specslužb" ["We must share!" or protection of personal data of Russians from foreign special services], *GARANT.RU*, http://www.garant.ru/article/559071/ (accessed: 27.04.2018).

[5] See: SEEDIG, "SEE Summary", May 2018, http://seedig.net/seesummary-may-2018/ (accessed: 9.07.2018). SEEDIG is a sub-regional Internet Governance Forum working in the region in cooperation with European Dialogue on Internet Governance and the Global IGF. In cooperation with the Geneva Internet Platform it provides monthly monitoring of the legislation within the region that is useful to analyze the state of the national legislative initiatives regulating the Internet.

Human rights issues and restrictive measures

In Russia it is necessary to designate creation of the number of registries of domain names and page indexes on the Internet containing information prohibited for dissemination in the Russian Federation. This law introduced so-called blacklists.[6] These are sites which contain information initially relating to three categories: propaganda of pedophilia, drug addiction and suicide.

The Russian Association of Electronic Communications in relation to this law emphasizes the possible negative consequences of the application of this law. Among these is the blocking of bona fide resources located on the same IP address as the resource holding illegal content, etc.[7]

In other words, in this case we can see the possibility of outrageous decisions of blacklist operators. Besides, those blacklists were introduced on the basis of the decree of the government (not the Federal Law),[8] while according to the Russian Constitution rights and freedoms may be restricted only by a court and on the basis of Federal Law. In this case, this principle is violated.

It should also be noted that it is not suitable to block resources from a technological viewpoint. Thus, even before the introduction of blacklists there was the decision of the court, the result of which was that access to the LiveJournal blog-platform was partially blocked in Russia.[9]

On Friday, June 24, 2016, the State Duma passed a package of "anti-terrorist" amendments to the legislation, developed by deputy Irina Yarovaya and member of the Council of the Federation Viktor Ozerov (hereinafter the Yarovaya Law). After the first reading some of the most resonant bill norms were relaxed or removed, but the document remains a significant part of the provisions criticized by the IT sector.

The Yarovaya Law obliges telecoms operators and Internet companies to store text messages to users, their conversations, as well as "the image, sound, video and

---

[6] See: Federal Law No. 139-FZ of 28.07.2012 (as amended on October 14, 2014) "On Amendments to the Federal Law", "On Protection of Children from Information Harmful to Their Health and Development" and certain legislative acts of the Russian Federation (ConsultantPlus Legal Reference System).

[7] See: RAEC position on the initiative of the Safer Internet League, http://raec.ru/live/position/5898/ (accessed: 27.04.2018).

[8] See: Resolution of the Government of the Russian Federation No. 1101 of October 26, 2012 (edited on 12.10.2015) "On the Unified Automated Information system 'Unified register of domain names, indexes of pages of sites in the information and telecommunication network "Internet" and network addresses, allowing to identify sites in the information and telecommunication networks "Internet" containing information, the dissemination of which is prohibited in the Russian Federation'" (ConsultantPlus Legal Reference System).

[9] See: A. Golitsyna, V. Kholmogorova, M. Galkin, "ŽŽ častično nedostupen" [LJ is partially inaccessible], *Vedomosti*, 26.06.2009, no. 116, https://www.vedomosti.ru/newspaper/articles/2009/06/26/zhzh-chastichno-nedostupen (accessed: 27.04.2018).

other communications" up to six months. How exactly and how long the information will be stored, should be defined by the government. In addition, operators will have three years to store information on facts of receiving, transmission, delivery and processing of messages and calls. Operators will be obliged to provide access to all these information to the law enforcement authorities without a court order.[10]

According to the amendments, network operators must retain information on the facts of receipt, transmission, delivery and (or) processing of voice and text messages, including their contents, as well as images, sounds, or other users' communications and provide the authorized state bodies conducting operational and investigative activities, or maintaining the security of the Russian Federation, information about the users of communication services and provided services of communication and other information necessary to carry out tasks on these bodies, in cases established by federal laws.[11]

In addition, it is necessary to pay special attention to the impact on the constitutional rights and freedoms of citizens of the so-called Yarovaya Law. As described, these amendments provide disclosure of personal data to the competent authorities. On the first stage it is the statistics for each user's traffic, on the second stage it is decrypted transmitted data (messages and so on.). Thus, third parties (employees of state bodies) become aware of the privacy of citizens, their correspondence and other data, access to which of any third party other than the addressee would be banned or at least restricted under normal circumstances.

In Ukraine, a draft law on counteracting threats to national security in the information sphere is on the agenda in the country's parliament. The draft law was introduced in parliament last July and it proposes amendments to several existing laws. The proposal would broaden the concept of technological terrorism, to cover acts conducted via the Internet and other global networks for data transmissions with aims such as violating public order, intimidating the population, provoking armed conflict, aggravating international relations, or "attracting public attention to political, religious or any other views of the perpetrator (terrorist)." It would also allow for temporary (up to 48 hours) denial of access to online content without a court order, at the request of a prosecutor, investigator, or the National Council for Security and Defense. A court order would still be required after a temporary block is put in place. Human rights groups have raised concerns about the provisions, worried about possible abuses from the authorities in interpreting the definition of technological terrorism and in imposing temporary blocking measures.

[10] See: E. Arkhangelskaya, A. Sukharevskaya, "Kod Ârovoj: čem grozit antiterrorističeskij zakon internet-pol'zovatelâm" [The Yarovaya code: The threat of an anti-terrorist law to Internet users], *RBC News Agency*, https://www.rbc.ru/technology_and_media/24/06/2016/576c0a529a79471b-c44d2b57 (accessed: 27.04.2018).

[11] See: Draft Federal Law No. 1039149-6 "On Amending Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Measures to Counter Terrorism and Ensure Public Security". Submitted to the State Duma of the Federal Assembly of the Russian Federation, text as of 7.04.2016 (ConsultantPlus Legal Reference System).

As the Internet is becoming a more and more powerful source of information, the Belarussian government is using different methods to keep it under control.

The first method is control over the technical infrastructure. Beltelecom, a state-owned telecommunications company, has a monopoly over the country's external Internet gateway, and the previously-announced plans to open up international connections to other operators were eventually put on hold.

Second of all, there is legislation in place that regulates the activities of Belarusian citizens on the Internet. One of the most important pieces is Presidential Decree No. 60 of February 1, 2010, "On Measures to Improve the Use of the National Segment of the Internet". Today, it is the most notorious legislative act to provide the state with tools for online surveillance and censorship. But in fact, even before the decree was introduced, there were legal mechanisms that affected free speech online in the country.

In 2008, a new media law first introduced the notion of online media, but it gave no clear definition of what it is, and there is still none. No further governmental decree on the regulation of online media has ever actually been published, despite the law being in force for five years.

The regime has effectively used laws aimed at offline media in an attempt to curtail online media in Belarus — in particular the articles of the criminal code on defamation. It is a crime in Belarus to insult a state official — and the most serious such offence, punishable with up to five years in prison, is defamation of or insulting the president. In 2007, the writer and opposition activist Andrey Klimaw was sentenced to two years in prison for publishing critical articles on the Internet. He was later released in 2008. The journalist Andrzej Poczobut was convicted of libeling the president in July 2011 and given a three-year suspended jail sentence for articles and blog posts he published online.[12]

In early 2018, a draft law amending media legislation is currently being discussed in parliament. The bill, which passed its first reading in the House of Representatives of Belarus, would directly affect online media. Although not compulsory, online media would need to register with the authorities to enjoy the benefits of traditional media (such as obtaining media accreditation and information from state bodies). The bill would also introduce a series of obligations for owners of Internet resources, such as monitoring the content so as not to allow the distribution of illegal material. Moreover, the Ministry of Information would be able to decide on restricting access to certain online resources. The bill is seen by human rights organizations as a threat to freedom of the media and freedom of expression. The government did not rule out the possibility of the current draft being substantially modified in the light of ongoing debates.[13]

[12] See: A. Aliaksandrau, "How free is the Internet in Belarus?", [in:] *Digital Eastern Europe*, eds. W. Schreiber, M. Kosienkowski, Wrocław 2015.

[13] See: SEEDIG, "SEE Summary", April 2018, http://seedig.net/seesummary-april-2018/ (accessed: 9.07.2018).

Harlem Désir, Representative on Freedom of the Media of the Organization for Security and Co-operation in Europe (OSCE) sent a letter to Turkey's Foreign Minister Mevlüt Çavuşoğlu outlining concerns about the detention of social media users in Turkey. According to Turkish authorities, 449 individuals were arrested on claims of spreading terrorism propaganda after writing in social media about Turkey's military operations in Afrin, Syria. Désir called on Turkey to reconsider its practices and allow individuals to exercise their right to freedom of expression and express dissenting views on social media. "Disagreeing with actions taken by the government should not be punished with imprisonment. Freedom of expression must be respected, even in times of conflict or war", he noted.[14]

In the case of Ahmet Yildyrym vs. Turkey the applicant appealed against judicial blocking of the service of creating and hosting Google sites, where he published various materials, including his own scientific works. The European Court noted that the blocking of a separate website containing violations was based on legislation, but neither the applicant's site nor Google sites in general fell within the scope of the relevant law. While Google's service Sites was responsible for the content of the site posted on it, the law did not provide for blocking general access to the service. From the point of view of the European Court of Justice, the general blockade made large amounts of information inaccessible, thus "making large amounts of information inaccessible, significantly restricting the rights of Internet users and leading to significant indirect consequences" (§ 66 of the Decree). Thus, the European Court found that there had been interference with the right to freedom of expression.

In 2014, the European Court adopted a decision in the case of Akdeniz vs. Turkey,[15] in which the applicant, who was a regular user of myspace.com and last.fm, appealed against their blocking. Access to sites was blocked due to the dissemination by the latter of music works in violation of copyright. Despite the inadmissibility of the applicant's complaint for consideration on the merits, the European Court recognized "the paramount importance of the rights of Internet users", since it is the Internet that is the most important means of exercising freedom of expression. Consequently, the regulation of Internet access should be in accordance with the requirements of Article 19 of the Universal Declaration of Human Rights of 1948 and provisions of international law.

The subject of the Internet has found its reflection in the case-law of the European Court of Human Rights. In 2017, the European Court considered the case Yan-

[14] See: SEEDIG, "SEE Summary", February 2018, http://seedig.net/seesummary-february-2018/ (accessed: 9.07.2018).

[15] See: Judgment of the European Court in the case of Yaman Akdeniz vs. Turkey (Yaman Akdeniz vs. Turkey) of 11 March 2014, complaint No. 20877/10, as quoted by: A.S. Shatilina, "Human rights on the Internet: The problem of recognition of the right of access to the Internet", *Precedents of the European Court of Human Rights* 2018, no. 1, pp. 38–45 (ConsultantPlus Legal Reference System).

kovskis vs. Lithuania.[16] According to the circumstances of the case, the applicant petitioned the prison administration to grant him access to the Internet to obtain information about entering the university. However, his application was rejected, and the national courts upheld this decision unchanged. The country's courts noted that, despite the absence of a ban on the use of the Internet in the rules for keeping prisoners, telephones were included in the list of prohibited items. The essence of these restrictions was to prevent the committing of new crimes by prisoners. Guided by this, the courts of Lithuania came to the conclusion that the ban on the use of the Internet has a similar purpose. The Supreme Administrative Court upheld the decisions of the lower courts. He noted that not a single law regulating the rights of prisoners enshrined the right to access to the Internet. The domestic court also pointed out that providing access to the Internet would have a negative impact on the fight against crime, since it would make it difficult to monitor the movements of prisoners. However, the Court held that there had been a violation of Article 10 of the Convention in the present case. Since Lithuanian legislation guaranteed access to information related to education, restriction of access to the relevant Internet site constituted an "interference with the right to receive information that was not necessary in a democratic society". The European Court noted that the decisions of the domestic authorities were focused on prohibiting prisoners from accessing the Internet, and not on the fact that access to a particular Internet site was necessary for education. The Lithuanian authorities also did not consider the possibility of providing controlled access to a particular site owned by a government agency. The European Court recognized that the Internet plays an important role in people's daily lives, in particular because certain information is available only on the Internet. Thus, Article 10 of the Convention cannot be interpreted as imposing a general obligation to provide prisoners with access to the Internet.

Attempts at establishing national regulatory frameworks

Since 1999 Bulgarian telecom laws have established a long tradition of lacking any regulation, or even registration for Internet services, and domain names and IP addresses are left outside of the regulatory framework. These Internet-friendly texts in the Law for Electronic Services have not been changed since the case that the Internet Society of Bulgaria filed in 1999 against the government's desire to implement licenses over Internet Service Providers. Most recently the attitude of

[16] See: Resolution of the European Court in the case Jankovskis against Lithuania (Jankovskis vs. Lithuania) on January 17, 2017, the complaint No 21575/08, *Bulletin of the European Court of Human Rights* 2017, no. 6.

the government towards Internet governance was explained in the signed Memorandum of Understanding between the Ministry of Transport, IT and Communications and ICANN, where there is text, recognizing the multi-stakeholder model of governance of the Internet.[17]

After legalizing cryptocurrency transactions, Belarus has taken another step in the regulation of blockchain technology. Alexander Lukashenko, the Belarussian president, issued a presidential decree which regulates businesses based on blockchain technology and legitimizes smart contracts at the state level. The new law also exempts technology companies from certain taxes and allows better cooperation with foreign banks.[18]

The Turkish parliament has passed a law that will put online streaming platforms under the same regulations as those applicable to radio and television services. The law provides that "institutions wishing to stream radio and television content only over the Internet" are to "receive a license for only this purpose". This way, online broadcasts will be subject to the same content supervision by the country's Radio and Television Supreme Council (RTÜK) as those transmitted via landline, satellite, and cable. RTÜK could report unlicensed transmissions to a criminal court, asking for their ban.

Lawmakers in Armenia are proposing legislation to legalize cryptocurrency-related activities. A draft law on the development of digital technologies has been put forward in the country's parliament, and one of its aims is to liberalize the cryptocurrency industry, by eliminating "unnecessary bureaucracy" and "avoiding monopolization". If adopted, the law would introduce tax exemptions and other incentives for miners and allow individuals and businesses to operate mining facilities without the need to apply for any special licenses or permits. Miners would be exempt from taxation until the end of 2023. Proponents of the draft law, who took inspiration from similar regulations in countries like Belarus and Estonia, noted that the cryptocurrency industry should be encouraged and supported with legislation, as it could be a source of revenue for Armenia.[19]

In Albania, the Ministry of Health and Social Protection, the Ministry of Education, Sports and Youth, and the Ministry of the Interior approved a National Action Plan of Child Online Safety for the period 2018–2020. The plan, prepared with the support of the Children's Human Rights Centre of Albania, aims to increase child safety online by strengthening the capacities of national and local institutions, consolidating partnerships between government institutions, civil society, and the private sector; and strengthening the relevant legal framework and awareness policies. At a launch event, participants stressed the importance of multi-stakeholder

[17] See: M. Yakushev, V. Markovski, "Internationalizing Internet Governance in Eastern Europe", [in:] *Digital Eastern Europe*, eds. W. Schreiber, M. Kosienkowski, Wrocław 2015.

[18] See: SEEDIG, "SEE Summary", June 2018, http://seedig.net/seesummary-june-2018/ (accessed: 9.07.2018).

[19] See: SEEDIG, "SEE Summary", February 2018.

cooperation in the area of child safety online and outlined challenges in protecting children from cybercrimes such as online abuse and exploitation.[20]

So, according to Thorbjorn Jagland, Secretary General of the Council of Europe, the Internet, as a rule, is accessible to the majority of citizens in member states. The available data demonstrate a stable positive situation in almost half the member states, and most countries provide open access to the Internet. Despite the increasing spread of broadband access, in some member states the lack of access to the Internet remains critical. In addition, there are significant differences with regard to the proportion of the population using broadband access, even in open access Member States.

Limitations of Internet content, as a rule, are provided by law. In most Member States, the rules that apply to offline media are distributed to online media. Several states have introduced special rules for the regulation of illegal content distributed over the Internet. In six Member States, data show a worsening of the situation, as restrictions on freedom of expression online are not clearly defined in the law. Arbitrary restrictions on freedom of expression may arise, in particular, if the grounds for restricting or filtering online content are ambiguous and broad, for example, using terms such as "humiliation of national dignity", "extremism", "terrorist propaganda" or "justification of terrorism".

In most Member States (here we should mention that Belarus is not a member state of the CoE), public authorities refrain from filtering or blocking online content in an arbitrary manner and ensure that all content restrictions are based on decisions of a judicial authority or an independent body. Some Member States have created new bodies that play a leading role in content restrictions or removal from the Internet, based on specific rules specifically designed for the online environment. This may raise concerns about the independence of such bodies and their impact on freedom of expression.

Regarding the regulatory framework that affects Internet mediators and their responsibility for the dissemination of online content, Member States typically use similar approaches: intermediaries are not responsible for posting information disseminated through the technology they provide unless they are aware of the illegality of content and do not take urgent measures to remove it. However, the interpretation of this rule is not the same in all states. Member States, for example, have adopted different approaches to what qualify as "knowledge" and "immediate removal", and there are various procedures that can lead to the elimination of illegal online content. Although the European Court of human rights usually indicates that Member States have a wide margin of appreciation in assessing whether, or what measures must be taken to pursue a legitimate aim that can justify restrictions on freedom of expression, the lack of a common approach entails uneven levels of protection for freedom of expression in Europe.

[20] See: SEEDIG, "SEE Summary", March 2018, http://seedig.net/seesummary-march-2018/ (accessed: 9.07.2018).

Various legislative initiatives by Member States have increased the possibilities for overseeing the communications of Internet users. At the same time, the situation in most Member States of the Council of Europe clearly remains unchanged from 2015, when there was little data on supervisory activities for commercial, political or other purposes, the very fact that the most advanced technologies are used for mass monitoring of communications with prevention of accidents can be problematic. The European Court stated in January 2016 that this legislation should provide sufficiently accurate, effective and comprehensive guarantees for the acceptance, execution and potential reimbursement of such measures in order to avoid abuse. Most importantly, strict judicial control must take place at all stages of the process, from authorization to the application of supervision measures, even if only emergency situations can allow only judicial review *ex post facto*.[21]

Proposal of the international regulations

Here we can consider the draft of the international human rights treaty on the Internet, which was developed by a student project from the Faculty of Law of the Higher School of Economics on the assignment of the author of this article. The provisions of this agreement may be submitted as a proposal to regulate the Internet on the international global and regional levels.

This international agreement is expected to guarantee access to the Internet as a human right, and the right to seek and freely receive, transmit, produce and disseminate information on the Internet in any legal way. In this case, the restriction of access to the Internet or any part of it for the entire population or for certain segments (Internet disconnection) should be completely prohibited, as well as delaying operations on the Internet as a whole or some part thereof for the whole population or for certain segments of it. It is obvious that regulating the Internet through registration on certain domains is not a limitation of Internet access.

The states that have acceded to this agreement should promote universal access to the Internet, in particular to create legislative mechanisms that imply the development of an infrastructure that allows everyone to have access to the Internet, to create Internet communities based on local communities that allow Internet resources to be used openly, to provide support for Internet connections when necessary, to promote the improvement of Internet literacy of the population, to inform the public about the availability of a foundation the right to access the Internet, and to take special measures to achieve equality in the right to access the Internet.

[21] See: T. Jagland, "On the state of democracy, human rights and the rule of law", *Precedents of the European Court of Human Rights* 2018, no. 1, pp. 5–11 (ConsultantPlus Legal Reference System).

Access to the Internet should be guaranteed without any discrimination and guarantee equal rights of access to it. In the distribution, traffic and data on the Internet there should not be any discrimination regarding race, skin color, gender, language, religion, political or other opinion, national or social origin, property, birth or other status. Also, there should be no discrimination based on the class of device, content, authorship, origin and/or destination of publications, services or applications.

Each user must be equally protected from all forms of crimes committed via the Internet and should be entitled to a secure connection to the Internet.

According to the protection of freedom of opinion and expression each person should have the right to distribute and receive information through an Internet connection, including the lack of censorship must be guaranteed.

Each user must be eligible for Internet protest, which implies the right of everyone to participate in live and online protests.

The Internet should be prohibited from filtering and blocking, if this results in limiting or slowing down legitimate operations on the network. If content filtering and blocking takes place lawfully, users should have the right to know all the criteria used to restrict access, which should be enshrined in legislation, as well as published on the official website.

User rights should be limited only by a court decision, and users must also be able to appeal, that is, they must have clear, convenient and accessible stages of the appeal mechanism. All other restrictions must be regarded as forms of censorship and are not allowed.

From the point of view of protection of the freedom of assembly and association each person should have the right to participate freely in various groups and associations and in the Internet, including the right to join, meet, join groups and create network meetings at any time.

From the point of view of privacy each user must have the right to privacy in the network, to privacy of correspondence, negotiations and other forms of online communication. The policy of the state on Internet privacy should be clearly stated and be in convenient and quick access to the resources available to each person. Everyone should have the right to inviolability of their virtual personality.

Everyone should have the right to use encryption technology to ensure secure, private and anonymous communication on the Internet as well as communicate freely, without arbitrary surveillance or eavesdropping, and without the threat of surveillance or interception.

Each user should have the right to protect honor and dignity on the Internet, as well as protection against slander.

From the perspective of personal data protection, when requesting personal data, the requestor is required to obtain the informed consent of the persons whose data concerns the request. Informed consent includes information about the content, purposes, storage locations, access mechanisms, as well as search and

modification of personal data. Control over the protection of personal data must be carried out by an independent monitoring body.

From the perspective of the right to take part in Internet governance each person should have the right to equal participation in Internet governance at all levels, including the right to access and to e-services and participation in e-government.

* * *

A brief overview of the national legislative initiatives in considered European states shows us that the most problematic area is non-compliance of national legislation regulating the Internet with international and regional standards in Internet governance. Some countries, including Russia, are providing restrictive measures incompatible with the human rights of Internet users.

The very international rules are formulated as soft law rules, which are not obliging states to comply with. This is a general problem of international rules regulating the Internet. The European Union legislation looks like the exception from this, but European Union legislation is only in force in its Member States. For non-EU states this legislation could be a model law to comply with, because we could conclude that standards of human rights protection are higher than outside.

This outlines the need for proclamation of international regulations both on the universal and regional European levels. There are two basic values that we need to preserve by proclaiming international regulations. The first is integrity of the Internet, bearing in mind attempts for fragmentation on national levels. The second is human rights protection which should be the key issue for each international legal act.

Bibliography

Aliaksandrau A., "How free is the Internet in Belarus?", [in:] *Digital Eastern Europe*, eds. W. Schreiber, M. Kosienkowski, Wrocław 2015.

Arkhangelskaya E., Sukharevskaya A., "Kod Ârovoj: čem grozit antiterrorističeskij zakon internet-pol′zovatelâm" [The Yarovaya code: The threat of an anti-terrorist law to Internet users], *RBC News Agency*, https://www.rbc.ru/technology_and_media/24/06/2016/576c0a529a79471b-c44d2b57 (accessed: 27.04.2018).

Filimonov A., "'Delit′sâ nado!' ili Zaŝita personal′nyh dannyh rossiân ot inostrannyh specslužb" ["We must share!" or protection of personal data of Russians from foreign special services], *GARANT.RU*, http://www.garant.ru/article/559071/ (accessed: 27.04.2018).

Golitsyna A., Kholmogorova V., Galkin, M., "ŽŽ častično nedostupen" [LJ is partially inaccessible], *Vedomosti*, 26.06.2009, no. 116, https://www.vedomosti.ru/newspaper/articles/2009/06/26/zhzh-chastichno-nedostupen (accessed: 27.04.2018).

Jagland T., "On the state of democracy, human rights and the rule of law", *Precedents of the European Court of Human Rights* 2018, no. 1.

Kurbalija J., *An introduction to Internet Governance*, 7th ed., Geneva 2017.

Shatilina A.S., "Human rights on the Internet: The problem of recognition of the right of access to the Internet", *Precedents of the European Court of Human Rights* 2018, no. 1.
Yakushev M., Markovski V., "Internationalizing Internet Governance in Eastern Europe", [in:] *Digital Eastern Europe*, eds. W. Schreiber, M. Kosienkowski, Wrocław 2015.

Legal sources

Convention for the Protection of Individuals with Automatic Processing of Personal Data. It was concluded in Strasbourg on 28.01.1981 (ConsultantPlus Legal Reference System).
Draft Federal Law No. 1039149-6 "On Amending Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Measures to Counter Terrorism and Ensure Public Security". Submitted to the State Duma of the Federal Assembly of the Russian Federation, text as of 7.04.2016 (ConsultantPlus Legal Reference System).
Federal Law No. 139-FZ of 28.07.2012 (as amended on October 14, 2014) "On Amendments to the Federal Law", "On Protection of Children from Information Harmful to Their Health and Development" and certain legislative acts of the Russian Federation (ConsultantPlus Legal Reference System).
Federal Law No. 242-FZ of July 21, 2014 "On Amendments to Certain Legislative Acts of the Russian Federation Regarding Specifi cation of the Procedure for the Processing of Personal Data in Information and Telecommunication Networks" (as amended on December 31, 2014) (ConsultantPlus Legal Reference System).
Judgment of the European Court on the case of Ahmet Yıldırım v. Turkey of 18 December 2012, complaint No. 3111/10.
Judgment of the European Court of Human Rights on the case of Yaman Akdeniz vs. Turkey (Yaman Akdeniz vs. Turkey) of 11 March 2014, complaint No. 20877/10.
Judgment of the European Court of Human Rights on the case of Jankovskis against Lithuania (Jankovskis vs. Lithuania) on January 17, 2017, the complaint No 21575/08, Bulletin of the European Court of Human Rights 2017.
Resolution of the Government of the Russian Federation No. 1101 of October 26, 2012 (edited on 12.10.2015) "On the Unified Automated Information system 'Unified register of domain names, indexes of pages of sites in the information and telecommunication network "Internet" and network addresses, allowing to identify sites in the information and telecommunication networks "Internet" containing information, the dissemination of which is prohibited in the Russian Federation'" (ConsultantPlus Legal Reference System).

Online sources

RAEC, http://raec.ru/live/position/5898/ (accessed: 27.04.2018).
SEEDIG, "SEE Summary", April 2018, http://seedig.net/seesummary-april-2018/ (accessed: 9.07.2018).
SEEDIG, "SEE Summary", February 2018, http://seedig.net/seesummary-february-2018/ (accessed: 9.07.2018).
SEEDIG, "SEE Summary", June 2018, http://seedig.net/seesummary-june-2018/ (accessed: 9.07.2018).
SEEDIG, "SEE Summary", March 2018, http://seedig.net/seesummary-march-2018/ (accessed: 9.07.2018).
SEEDIG, "SEE Summary", May 2018, http://seedig.net/seesummary-may-2018/ (accessed: 9.07.2018).