National Research University
Higher School of Economics

Human Rights on the Internet:
Legal Frames and Technological Implications

Compendium on Internet governance

Volume 2

Moscow
2013

УДК 342.7:004
ББК 67.404
Н91

Н91 **Human Rights on the Internet**: Legal Frames and Technological Implications: Compendium on Internet governance. Volume 2 [Text] / ed. by S. Maltseva, M. Komarov and A. Shcherbovich; National Research University Higher School of Economics. – Moscow, 2013. - 92 pp. - 200 copies. - ISBN 978-5-7598-1112-1 (pbk).

This compendium comprises transcript of the workshop on 'Human Rights on the Internet: legal frames and technological implications' organized by the Higher School of Economics on the 7th Internet Governance Forum (Baku, Azerbaijan, 6–9 November, 2012) and relevant articles on legal and technological issues of Internet Governance in sphere of human rights, prepared by the group of legal and technical scholars of information studies of the Higher School of Economics. This compendium is devoted to the forthcoming 8th Meeting of the Internet Governance Forum on Bali, Indonesia, 22–25 October 2013.

УДК 342.7:004
ББК 67.404

ISBN 978-5-7598-1112-1

CONTENTS

WORKSHOP "HUMAN RIGHTS ON THE INTERNET: LEGAL FRAMEWORKS AND TECHNOLOGICAL IMPLICATIONS"

7th Meeting of the Internet Governance Forum, Baku, Azerbaijan, 8th November 2012

Background Paper

A cyberspace philosophy promotes maximum independence of the internet from any government and other forms of interference. It is impossible, however, to preclude any kind of internet governance or regulation thereof. The internet is like a mirror reflecting the real world, where we have moral and legal rules called to provide and ensure freedom of expression and information accessibility rights, protection from abuse of those rights by criminal and other kinds of wrongful behavior.

Similar rules should also exist in the cyberspace. Nowadays, we could in fact reveal the three levels of internet governance, namely: supranational, national and self-regulation. Due to the specificity of the internet, none of these levels could be declared self-sufficient or unique to set up relevant management rules. The main purpose of this paper is to compare these three levels of internet governance and to allocate their roles in this process according to their functional characteristics.

To sum up, we can outline the following positive aspects of internet governance at an international level:

- an open and unrestricted dialogue on internet governance issues, including the freedom of expression and information accessibility rights, independently from national legislation or ideology of certain states;

- 'participatory' approach, i.e. involvement of many actors in decision-making process, such as governments, international intergovernmental and nongovernmental organizations, scientific and professional community and other representatives of civil society dealing with the issues of internet governance;

- an open-minded, more complete and scientifically sound analysis of the issues of internet governance;

- an international level more adequately reflects the supranational nature of the internet as a worldwide information network 'without borders', which approaches the accepted rules to reality;

- due account of fundamental human rights instruments adopted by the United Nations and regional international organizations.

We can also show some weaknesses of the international level:

- in most cases the decisions of international organizations are of recommendatory nature, which prevents us from hoping that such decisions will be adopted by all jurisdictions at a national level with the exception of such regulations as international treaties that are properly signed and ratified by member states, like the European Convention on Human Rights (1950), the Budapest Convention on Cybercrime (2001), etc.;

- not all national jurisdictions unequivocally perceive particular international norms and principles of internet governance;

- most of the above proposed norms and principles of internet governance have ethical nature, which requires extremely high level of legal and information culture for them to be adopted in a particular country;

- many international non-governmental and intergovernmental organizations (Reporters Without Borders, IFLA, etc.) perceive any attempt to regulate the internet as an illegal establishment of censorship on the internet, which means an automatic denial of freedom of

expression and information accessibility rights of internet users.

Consequently, as for the supranational level of internet governance, the following should be stressed here.

- Development and launching of programs and policies aimed to improve internet governance theory, ideology and methodology.

- Arbitration, counseling, intermediary and other methods of dispute settlement between national jurisdictions in the sphere of internet governance.

- Development and promotion of ethical standards of internet governance, which includes the development and improvement of the Codes of Ethics at supranational (global and regional) and national levels.

- Clarifications and training courses aimed to promote internationally approved programs and policies of internet governance.

- Development of obligatory rules stipulated in multinational treaties and conventions designed to protect basic human rights in the sphere of information, such as the freedom of expression/speech and information accessibility rights, with due account of the cyberspace.

- Assistance in the ratification of such treaties and agreements and their implementation in national legislations.

- Monitoring of government abidance by the established rules of internet governance to guarantee the freedom of expression and information accessibility rights.

We can outline the following positive aspects of internet governance at a national level:

- as a rule, there are well-defined members of the regulatory process with a specific legally bound mandate to implement it 'traditional' and clear (understandable) mechanisms for protecting citizens' constitutional rights when they are violated (judicial, administrative, etc.);

- references to legislation and international law implemented by the country as a part of national legal system provide greater guarantee of legal protection of freedom of expression and information accessibility rights;

There are, however, certain weaknesses of internet governance at a national level:

- possible abuse of power by national security, law enforcement and state control officials in

the process of control or supervision exercised over the activities of internet service providers and the users;

- imperfect legislation that lags behind the level of development of internet technologies, including the lack of definitions of sufficient internet-related terms;

- users whose freedom of expression or information accessibility rights are violated would not sometimes seek to protect their rights with public authorities because of the fear of corruption or red tape;

- insufficient legal culture and legal literacy of many internet users prevents them from efficient defense of their rights by using state mechanisms of legal protection.

The national level of internet governance should be assigned for the compliance of following functions.

• Ratification of international treaties and conventions in the sphere of internet governance and their implementation into national legislation.

• Establishment of favorable legal environment for realization of freedom of expression and information accessibility rights in the internet, including modernization of national legislations according to the modern development of WEB 2.0 and other cutting-edge

technologies of cyberspace, especially the possibility to make user-generated content on websites.

- Protection of constitutional freedom of expression and information accessibility rights in the internet by judicial and administrative bodies in a statutory manner.

- Prevention of the abuse of information rights in the internet by imposing legal restrictions that are based on constitutional provisions for defending constitutional interests, such as health, morality, another person's rights, national defense and security.

Now, we would like to outline positive aspects of self-regulation of web resources:

- freedom of actions of individuals realizing information rights in the internet and ensuring that such rights are observed

- a possibility of diversification of regulatory policy, depending on the specific resource in the internet

- administration of an internet resource and the community of its users is voluntarily interested in compliance with the user agreement of the web resource

- establishment of a competent community of users of internet resources and their corporate culture with ethical norms, customs and rules of conduct.

Among disadvantages of self-regulation we could see the following:

- user agreements are clearly optional for the users, whereas the rules and sanctions imposed by the administrations can be easily avoided by registering multiple accounts;

- the quality of protection of the freedom of speech in the internet depends on the legal and information culture of users, the ways of their interaction with the resource administration;

- the possibility of subjective approach to the violation or compliance with the user agreements, depending on the policy of a particular resource;

- if an internet resource is registered in a foreign jurisdiction, it can give rise to a conflict of jurisdictions which manifests itself in impracticable application of translated versions of user agreements that are recognized as unofficial ones;

- the user agreements stipulate their optional nature for the administration of the resource, or

easy ways to amend such agreements unilaterally, without any consulting with the users of the website.

Self-regulation on web resources should be allocated with the following functions.

- Formation and development of social networks on different websites, establishment of user communities and improvement of their information literacy and legal culture.

- Elaboration of rules of conduct formalized in user agreements and the terms of service, their compliance with statutory standards.

- Settlement of disputes arising in a process of realization of the freedom of expression and information accessibility rights on different websites in a statutory order within users network communities, possible arbitration by means of specially appointed conflict commissions, moderators and managers of such web resources.

- Development of standard (community) rules of internet governance on specific websites, which have both ethical and legal nature.

In a big range of legal issues arising in connection with Internet Governance and human rights,

on the workshop we should revise the following main issues.

1. The need to streamline regulation. In our point of view, following a three-tier division of Internet governance (supranational, national, and community level) in order to realize freedom of expression and the right to access information, it is necessary to provide necessary conditions for participation of online communities in the governance on separate web resources. For that reason it is required to streamline regulation of the rules of behavior on these resources, and introduce strict system of monitoring.

2. Revaluation of the legal nature of user agreements. It is possible to challenge the civil-law nature of the user agreements. The realization of the freedom of expression and the right to access information on the Internet is undoubted constitutional law value. Civil law cannot settle number of public law by nature of social relations connected with the implementation of human rights and freedoms, if freedom of expression on the Internet could be considered in this context.

3. New understanding of jurisdiction in cyberspace. Cyberspace should be treated as separate jurisdiction with their own rules, which reflect its unique character. Internal rules were designed as horizontal, in

which the subjects of law are standing as their creators. Consequently, there is need for a new understanding of the Internet governance and territoriality in cyberspace.

4. Establishment of the web communities. In social networks and other sites hosting user-generated content, user agreements do not contribute to the establishment of competent user communities. In this case, the term ‘competent’ includes such community of users, which user agreements have links to legislation and universally recognized principles and rules of the international law, as well as clear procedures for resolution of disputes by the appointment of responsible persons in an open and democratic manner. in this context it is also required to increase level of legal and information culture of users and administration of web resources.

5. Revision of the standards of responsibility. Rules on liability in the Internet, which existed in the era of ‘static’ web, should be reconsidered, because of the significance of the user-generated content. Resource owner is often just provides technical conditions for the activities of users. Thus, the responsibility of the owner of the resource is his need to establish rules of the website, to draft such rules for discussion of interested stakeholders, and comply with the conditions for their implementation. These rules shall not conflict with the law and impede the realization of

the freedom of expression and the right to access information on the Internet. The administration of the resource is an intermediary between the owner and resource users. Its main task is monitoring of the implementation of user agreements, avoiding abuse of the freedom of expression and the right to access information on the Internet.

From technological point of view we could outline the following issues affecting human rights.

1. Anonymity. The conflict of human rights concerns the issue of anonymity on the Internet. On the one hand the legitimate desire of the person to remain anonymous is understandable, but on the other hand, such freedom should be determined by the principle of non-violation of the rights of others. As on the Internet it is difficult to identify a person as this is due to technological features, there are quite a reasoned opinion on the prohibition of all anonymous to human activity.

2. Harmful Information. The spread of harmful information in the internet environment affects human rights, as each state understands by this category of their information. In this regard, there are situations in which you can avoid liability. In addition, in this area there is a problem of identification of offenders. Interaction of states could resolve such questions.

3. Electronic Courts. It creates a procedure for resolution of the dispute to the court in the application of electronic methods of conflict resolution together with the use of Internet technologies. The development of this technology will allow implementation of human rights on all the levels related to business and other economic activities. At the same time maximum use of modern information and telecommunication technologies.

List of Participants

Dr. Svetlana V. Maltseva, Dean of the Business Informatics faculty, National Research University Higher School of Economics, Moscow, Russia (Technical and Academic Communities).

Dr. Anna K. Zharova, assistant professor, Business Informatics Faculty, National Research University Higher School of Economics, Moscow, Russia (Technical and Academic Communities).

Andrey A. Shcherbovich, lecturer of the department of the Constitutional and Municipal Law, faculty of law, National Research University Higher School of Economics, Moscow, Russia (Technical and Academic Communities).

Dr. Jeremy Malcolm, Consumers International, Malaysia.

Dr. Wolfgang Kleinwaechter, University of Aarhus, Germany.

Roxana Radu, Graduate Institute of International and Development Studies, Switzerland.

Transcript

DR. S. MALTSEVA: Ladies and gentlemen, let's start the workshop "Human rights on the Internet: legal frames and technological implications". The initiative of this workshop belongs to the representatives of the academic community of Russian National Research University Higher School of Economics, Moscow. My name is Svetlana Maltseva, I'm acting dean of Faculty of Business Informatics of Higher School of Economics. And then, I will introduce the panellists from my right hand to the left. First of all, I want to introduce Wolfgang Kleinwaechter. He is a Professor of communication policy and regulation at the department for media and information studies at the university in Denmark. Then I want to introduce Jeremy Malcolm. Jeremy is senior policy officer for CI's Consumers and Project Officer for consumers in Digital Age. He is in Malaysia. Mikhail is a co-founder of

organisation Young Innovative Russia, Roxanna Radu is a Ph.D. candidate in international relations, political science at the Graduate Institute of International and Development Studies in Switzerland. Andrey Shcherbovich, and Anna Zharova from HSE. Unfortunately, Paul Vixie, the chairman and founder of Internet systems consortium will be later. The agenda of workshop include the session of reports of panellists and the session of questions and general discussion. You can see the agenda on the screen. For me, as for representative of academic community the main idea of this workshop seems to be a synergy effect of collaboration between the representatives of different areas of knowledge to provide new ideas in the field of providing human rights.

Also, we organised the remote session and I want to welcome the students and staff of Higher School of Economics, where this session is held. I want to welcome all of them, and to invite them to join us. Okay. So, we begin. I will start from our joint report with Mikhail, and, as you can see, now on the agenda, we'll move from technological problems to legal questions. First of all, I want to make short introduction to our report and then Mikhail will present the main ideas.

As you can see, the Internet technologists contribute to the practical realisation of human rights.

First of all, they can improve the effectiveness of exist institution, for example, E-learning. It is new for me as I'm a professor of the university. This type of training allows you to implement the rights to education for people who are unable to study in ordinary schools or/and universities. For example, people with disabilities. But you must ensure that the technology and content have the necessary quality, and user is protected from fraud. Also we can see the organisational transformation based on Internet technologies, and the emergence of new institution. Another example are social networks. We see that they can have a great impact on their forming and distribution of knowledge. Unfortunately, at the same time Internet technologies give rise to new mechanisms in terms of human rights violations. So we need to create new means, new technologies for protection. We need new restrictions including technological means, identification and classification of violations, prevention-based on predictive analytics. But what we really need to improve the situation is to improve the existing means, or we must build new models of communication. Perhaps, such model could be based on the concept of web 3.0, and I want to give the microphone to Mikhail, who will present our ideas about feasibility of it.

DR. M. KOMAROV: Thank you very much. Ladies and gentlemen, I would like to start with a

presentation about technological aspects of human rights.

So, dear colleagues, I would like to start the presentation about human rights and the Internet with some information from our past. It is necessary to emphasize the problem of protecting human rights appeared many years ago, when we became able to transfer data with the use of technical devices. As you can see on the slide, the first prototypes of networks were implemented in 1946, actually, 1947 directly with, you know, this physical prototype. Problem of protection of data is more serious, when we're talking about united technological networks, which are always vulnerable to the intrusions of third party technological devices or programmes. Human rights protection became more important and more vulnerable when we got the Internet more than 40 years ago as a concept, and, actually, as it started to be quite popular, I think almost 30 years ago, right? And the special actual problem appeared, when we got social networks and started uploading our personal and private data in our account in social networks truly believing that no one except us will be able to get our information from our account, even when it is tagged as “available only for me”. In terms of current technological progress, it is necessary to remind that almost 20 years ago there were only a few people around the world carrying cell phones. Nowadays, we've

cell phones everywhere, it is not a luxury thing but a necessity. The legal aspects of using cell phones are still on different stages of process depending on the different countries. Somewhere you need to show your passport or your ID, somewhere you can buy cell phone without any documents, which means that no one would know who is using that particular cell phone number and who transmits the data, actually.

At the same time, cell phones are sensors, and we're part of the big global telephone network which is much bigger than social networking. Before the smartphones, we were generally using just the phone functions of the cell phones but after their appearance, we have a small information bomb every day with us. Typical cell phone today has GPS, camera, Wi-Fi module and 3G, which means that it is easier to get your position, to see what you are doing with your cell phone and transfer all this data to the particular servers. This mobile area, which is called the Web 3.0 marks innovations of higher necessities. The new technology has a capability to supply more real-time content so this information comprises location, weather, traffic, local business and store frequencies, so this also provides new industry opening. No one can assure you, that you are safe using your cell phones, for instance, from the recent incidents it is necessary to remind about the incidents with iPhone or iPad devices, while they were recording

your position, or some other incidents, which still take place when you might be connected to the fake base station and pay additional money for the calls and text and transfer your personal data to them. Only from the recent times, some applications were proposed to check the base station. There are many examples of how our rights, actually, for the private life, for the privacy, were violated, and how companies can break into our privacy. The web concept has many different meanings, but all of them consider using information by the machines. Just Web 1.0, the information web, was straightforward enough. It was full of stated content that could be seen as an extension of offline media, such as TV. This version of the web was able to provide information to users in a broadcast model for information distribution. The next evaluation of the web brought about Web 2.0, or the social web, which is characterised by users' communications, contributing and collaborating. Web has empower users and customers of content and information into active producers of content and information. It allows users to equally participate in the production of content and sharing that content with the wider audience online. It means that our things, our belongings will have the power to learn, integrate and decide. Web 2.0 is a semantic web. It is a virtual environment of 3D Internet. Web 3.0 is a smart commerce and Web 3.0 is Internet of Things.

It is our future in terms of our life, but tomorrow in terms of how fast this technology will progress integrating new devices into our life. That's why it is necessary to focus on this aspect. Of course, you can see, you know, current solutions already implemented to protect our data and being able to filter in a proper content of the websites, Internet-based services for our children and, actually, ourselves as well. There are two main areas: hardware protection and software protection - which means that in terms of hardware, all of our data coming in and out of the PC or our devices connected to the Internet is filtered by special firewalls and hardware devices, and another area, software area, will be directly connected to the Internet with our PC or our mobile device and data, which is coming to our PC, is filtered directly on the PC and actually sometimes most of the time, we're managing that process.

It is quite hard to protect the data coming out of the PC this way, because we can assure ourselves that we've sent data to the particular address, and the data would pass through some other PCs or external services which means that, you know, our data might be protected only via special encryption systems. There are, of course, special legal act and regulations considering inappropriate use of our personal data in Russia. All the content providers must give access to the special services or special securities, you know, and in case of special

situations to the authorised representative of the governmental structures, but no one can assure you that your data are not be sent to the Internet just because we've got third party accessing your data, even in special cases. At the same time, all the Internet providers have all own filtration which means that they will be able to collect your emails, all the private information you are sending and receiving via the servers, and it is a good idea to focus your attention on the fact, that some Internet providers don't sign any legal documents saying that they wouldn't pursue data to the third parties. Of course, there are special providers of media or press in the Internet. They have to register themselves as special governmental structures. There is a special law saying that everyone dealing with personal information of someone should receive written confirmation, from the person creating the right to deal with that information. We also got special governmental black list of the websites or content providers, which regulates some particular websites. And there is, actually, no public discussions about the sites or content providers, which should be blocked. There is only governmental commission, which makes a decision. Right now, we are also in the process of implementing a special encryption services, personal encryption services and digital signature, at least to work with governmental organisations as E-government for the certification of data, which passes to the governmental structures.

We're talking about special regulation policies, about certification or special organisation, which probably should provide some special permission for the particular types of data, on the particular websites to secure our kids from inappropriate content. Web 3.0 is a semantic web, or Web of Things, lives according to the special rules. It should live, actually, according to the special rules provided by the certified association, probably as there should be a special improvement of the website, information on which should be somehow secured and approved. Also, we're talking about mobile networks. Services should be provided only after confirmation by the user and sending notifications to the user. In Russia, just recently we got the law, which regulates this. The same is for personal data protection by the law and special requirements to the databases. We've special databases and cloud-based services, keeping our personal data. So, there should be special protection laws and legal regulations about it. I would be happy to discuss it.

And there are also some ideas, how it might work in the future. As I said, in terms of technological progress our future is coming quite fast. So, there are some proposals what it will be like. In my opinion, we should consider our experience - it protects our personal belongings in terms of banking facilities, private storages, and also our personal data. There is some doubt

about granting access to the governmental organisations to personal data, probably there should be personal data officer, which would deal with particular people and particular people's data, at least we would know exactly the person, who would get access to our personal information, including our social status, banking accounts numbers, insurance numbers, et cetera. I would be happy to answer your questions, and, actually, during the question and answer session I would also like to ask you some questions. How we ensure synergy effect between new technologies and legal regulations in your opinion? I have my own opinion, I will tell about it later. And do you think there should be legal regulations to the services like hardware and software, which provide personal data in terms of amount or number of particular types of personal data, which is, for the enquiry, from the website, for instance. And another question, do you think there should be special improvement of the web sites for the Web 3.0 usage when we're talking about things using information from the web sites? Information should be reliable, but we should think about special regulations. Thank you very much for your attention.

DR. S. MALTSEVA: Thank you Mikhail. So, we can start the next report, Anna and Andrey will tell us about the problems of adaptation of the technological solutions to the changing legal environment. Andrey, you will be first, yes?

A. SHCHERBOVICH: Okay. Dear colleagues, my name is Andrey Shcherbovich. I'm a lecturer of the Higher School of Economics, and my colleague, Dr. Anna Zharova is associate Professor of the faculty of business informatics and we'll present together a report named “The adaptation of technical solutions to the changing legal environment”. Let's begin with the special concept of the Internet Governance, which was developed some years ago by a group from the Higher School of Economics, which is the trilateral model of Internet Governance. First, there are three levels on which Internet Governance should be possible: supranational, national, and community level or self-regulation. Those three levels couldn't be declared as self-sufficient, and should be connected to each other in the special way in order to make relevant Internet Governance, in order to make a model of IG policy in realisation of human rights.

So, each level has its positive and negative effect. None of them could be self-sufficient. At first, I will talk about the supranational level, which is like a multi-stakeholder approach of the IGF (Internet Governance Forums) and other forums and open discussion spaces provided by the United Nations, by the regional Internet Governance Forums and other organisations. It is also participatory approach, which everyone could be attended in discussion, and everyone have stock for

decision-making. It is also an open-minded and complete scientifically analysis of the problems of the Internet Governance, and also the Internet Governance itself better reflects on international level the supranational nature of the Internet itself. By the way, this supranational level on his own could have negative aspects, because it is the only discussion space, which have no decision-making official power to make international treaties, which have mandatory force. Also not all the national jurisdiction perceive their jurisdiction in the same way, so this recommendation could be recognised in different ways in different countries. Also most of the decisions and proposals made by such a discussion space are on the basis that has just ethical or not legal nature.

Other aspects are principal different position, which sometimes could not be in peace with each other: different organisations have different positions, for example on Internet filtering, on other issues like that, because of a lot of actors and stakeholders inside this process.

So, its functional assignment is development of the scientifically sound Internet Governance policy. It is counselling and sometimes promotion of ethical standards of regulation of making other rules, or like a proposal for international treaties and other, and also the monitoring of Internet Governance policies in realisation

of human rights around the world. Second national level is the Internet Governance, which is regulated by the national states. At first, the positive aspects are that they have a well-defined member and regulatory process within, and they are legally bound laws to implement it, and traditional and clear mechanism for protecting citizens by the normal judicial way. Also the normal national jurisdiction should use implemented at the national level rules and international law, which have a guarantee of realisation of human rights. But they also have negative aspects as other levels, so it is a possible to abuse the power by the law enforcement system of each country, it is in perfect legislation, which is absent for the real development of technologies. Also possible threats of corruption and red tape from national jurisdictions, in which protection of people could not be possible, and also insufficient legal culture, and legal literacy of Internet users in the field of protection of their rights on the Internet.

The special assignment of the national level is ratification of the international standards in the trading and convention on Internet Governance. It is established in a favourable legal environment, also protects constitutional rights and freedoms by traditional judicial and administrative bodies, and also prevents the usage of informational rights by legal restrictions based on constitutional provisions to prevent constitutional

interests as well as citizen, for example, morality, health, and other constitutional interests, national defence and security as well.

The third and the most controversial level of Internet Governance involved in the realisation of human rights and freedoms is community level. It also has positive and negative aspects. The community level is based on communities of, as a rule, big websites and web resources like Wikipedia, You Tube, Facebook and others, which have very competent communities of users. For example, these communities could have influence to the freedom of actions of individuals on websites, also possibility of diversification of regulatory policy in the independence of the website and its functioning structure. You can see other positive things, which are related to the community level of Internet Governance.

Negative aspects are that the user agreements, on which this level is based, are definitely optional for users. This level is very depending on the legal culture of users. Sometimes users of the major web resources are not really consistent with the real law and legal protection. Also there is the conflict of jurisdictions, because users are sitting in one place, one country, while website is registered in another country, administration of the website is sitting in a third country, and it is not possible to decide, which court is competent, have the

competent jurisdiction to protect our rights, if they were abused by the website administration. Also, as I said, those rules are very dependent on the ethics of users and their legal and informational culture. Its functional assignment is the major functional assignment of the community level of Internet Governance, the formation and establishment of the social networks on the different websites, elaboration of rules of conduction, and settlement of these views among users of different websites. For example, we've another situation when the illegal content is posted on the big website like the You Tube, for example, and the Court in Russia might have a decision to ban this website. All the website. For instance, it is better to go to contact the administration and, if possible, to delete this illegal content by decision of the administration, according to the internal rules of the web resource. Also the functional assignment of the community level of Internet Governance is the development of standard for rules of governance of different Internet resources, development of community of users and their legal informational culture. As well I said completing my part of the report, I would like to say that none of those levels of Internet Governance in the field of protection of human rights, couldn't be self-sufficient; all of them should be interconnected and interdependent with each other. Thank you. I would like pass the microphone to my colleague, Dr. Anna Zharova, who could explain the situation in Russia, and different

problems of the human rights and the Internet Governance arising in Russian legislation and jurisdiction.

DR. S. MALTSEVA: Thank you Andrey. Welcome, Anna!

DR. A. ZHAROVA: My second part is about particularly legal problems of the safety of the intellectual right in the Russian Federation. Constitution of the Russian Federation defines important right of citizen of Russia: the right to creative activity. It means that the State must provide to the citizen effective juridical remedies of those rights, but it doesn't mean that copyrights protection of the particular persons is the main activity for the government. Protection of the intellectual rights is connected with those legal mechanisms, which are provided by the legislation. Then, in the Russian Federation, lawmakers are facing the problems, which are presented on the slide. Point one. It is necessary that the subject of information relations must be identified as accurately as possibly because the subject existed not only in information relation. So other legal terms are considered in the Russian legislation.

Point two. The courts make damage assessment, but do they own it? The big problem of damage assessment of intellectual property placement in the

Internet is that it is connected with the technological possibilities to change frequency of visit of a site. All these problems prove the result of intellectual property was downloaded.

Point three. Every organisation makes rules of the estimation of damages caused by corruption of their intellectual property. A court is able not to consider their rules. Moreover, the court in each case actually should construct a forecast of economic efficiency of the invasion. For ensuring protection, it is necessary to have regulation. Rules of the relationship between provider, and user, and owner are not absent. However, in 2012 new article about creation of the register of forbidden sites was added to the Russian legislation. It was about child protection from harmful information.

Point four. After the extension of the Russian Federation to the WTO, the government of the Russian Federation decided to influence by fees to the invasion of foreign trademarks.

Point five. In Russia in 2011 new law was signed. This law facilitated confirmation of a right for intellectual property in the Internet.

Point six. Technical rules of the common direction, cybercrime in certain places are not affixed.

Point seven. Rules of realisation of online application use are not affixed. They are the experience of use of various technologies. This is in trial in Russian. That view accelerates this process of the reviewed resolution in the Internet. Thank you.

DR. S. MALTSEVA: Thank you Anna. I want to announce the next report that will do Jeremy Malcolm. He will present the report on the human rights and the future of Internet Governance. Please Jeremy.

DR. J. MALCOLM: Thanks very much. Well, the presentation so far have been very diverse so I'm going to restrict my remarks to the area that Andrey's presentation covered, which was about the different levels of Internet regulation, as he explained: the supranational level, the national level, and self-regulation, or regulation at the community level, as he called it, and I'm also drawing some of my remarks from my paper in this year's mind volume, which was edited by Professor Wolfgang Kleinwaechter. So the Internet Governance can be handled at the global level and that's obviously true, but we cannot be completely free to regulate at the national level, where human rights are concerned, because human rights are inherently global. The universal declaration of human rights was established as a global instrument precisely, because the national democratic process is not sufficient by itself to ensure that an individual country will respect human

rights within its borders. This is because by definition democracy means majority rule, and sometimes the majority does not wish to respect the human rights, particularly of minorities or foreigners. So, for example, freedom of expression is the freedom to speak out when the majority wishes you wouldn't, and would shut you up, if they could. The same is true for human rights in general. There are protections against the revolts against democratic majority. So, what this means is that even democratic governments may not always be inclined to protect human rights in the absence of international or supranational pressure. So, that's one important reason, why we establish human rights standards at the supranational level. But the national level sometimes comes back in because human rights are not always 100% culturally neutral. A good example of this recently came up with the tension between freedom of expression and the regulation of hate speech in the case of the anti-Islamic film “The innocence of Muslims”. The universal declaration does not have much to say about this sort of situation partly because the Islamic world had little input into the original drafting of the universal declaration. So does this mean that we should have regional or national human rights instruments rather than global ones? My answer is no. Largely in the case of the Internet, because the Internet doesn't operate that way. We've no borders online. So, acts that are conducted in one jurisdiction often spill over into other jurisdictions, particularly

where the Internet is concerned. So we've to try and make the regulation of the Internet work for human rights at a global level first and foremost, and only regulate at a national or regional level, when we've to in order to avoid culturally unjust outcomes. And to minimize the overreaching potential of such national or regional policies, it is important to fully exhaust the potential for the development and application of principles at a supranational level before an edge case devolves to the domestic level for cultural or other reasons.

So, in the case of the hate speech and defamation of religion, this means that we would have a global default regulation, which is freedom, because that respects the human rights of the greatest number of Internet users worldwide, and only where that falls down in particular cultures we have to look at allowing a national level override the global default policy.

So who decides on this? In the case of "The innocence of Muslims" video, who decided whether it would be available or not? It was Google. Now that's obviously not appropriate in the longer term. Google necessarily decided on this in a bad way, because they are a for-profit company. They may be a for-profit company that wishes not to be evil, but that's beside the point, right? Respecting human rights is something that they do because they happen to be a good corporate

citizen not because there is any global instrument that applies to them that they are morally or legally bound to comply with.

So this points to the fact that we cannot rely on individual governments to respect human rights, we cannot rely on corporations to do so, and civil society, well, certainly we can act as a human rights watchdog and we can provide certain tools to help with the exercise of human rights online, but we've nowhere near enough power or resources or influence to make much of a difference on our own account. So, how do we regulate the Internet in a way that respects human rights, if we cannot rely on governments, corporations or civil society to do so? The best answer we've is that we should do so by combining the strengths and weaknesses of all those stakeholders in a multi-stakeholder policy stakeholder policy development process intended to explicate common principles or guidelines upon which governments, the private sector and civil society can agree as a basis for their respective actions. Such as passing legislation, or concluding treaties, moderating online services containing user-generated content, and share norms of online behaviour.

The Internet Governance Forum can be a good place to start developing global policies for human rights online, particularly in areas, where there are no other global forum that have responsibility for particular

issues, such as, for example, privacy and cloud services. However, the IGF, as it is currently constituted, is not quite up to the task. Its mandate does call on it to develop recommendations on emerging issues that can be transmitted to decision-makers through appropriate high-level interfaces, but it hasn't yet developed the capacity to do that. And the agenda, furthermore, calls for a parallel policy to enhance co-operation on Internet policies, involving all stakeholders in their respective roles, and led by governments. So we've some more work to do to improve the processes at the global level, and we also have to make sure that similar forum exist at the regional and national levels too. In this context, it has been good to hear at this Internet Governance Forum, that there will be another attempt to convene a Working Group on enhanced co-operation under auspices of commission on Science & Technology for development. The ultimate outcome that we should be aiming for is to ensure that we've the means to address at all levels, supranational, national and local, the means to work towards a multi-stakeholder consensus on the appropriate principles to be applied by all stakeholders in their respective roles that will address online policy problems, while upholding human rights. Thank you.

DR. S. MALTSEVA: Thank you Jeremy. Our next report will do Roxana Radu. “Dynamics between

Internet Governance and human rights at the international level". Please, Roxana.

R. RADU: Thank you. While there is some consensus on what the international arena might consist of, I think, there are still some people who would question whether human rights are universal and whether socialisation into these international norms can actually make it possible that they become universal. The intersection of human rights with Internet Governance is itself an emerging topic and these processes are developing as we're speaking right now, and this is what makes this workshop very timely and I hope we can get something out of it that would enhance the discussion further on. I would like to point out a couple of tensions we need to take into account in actually moving forward with this debate. First, I would start by outlining the issue of interpretation. One of the questions that comes up first is whether regime treating the human rights in a comprehensive way, in a comprehensive manner as the so-called package of intersecting rights, or whether to keep the rights separated and have this list of independent things. We already have several core legal instruments in place at the international level, but their interpretation is uncontroversial. Access to Internet, for example, as a human right has been derived from several articles of the universal declaration of human rights, such as Article 2 on equality, Article 19 on freedom of

expression, or Article 26 on education. Secondly, the international human rights regime remains strongly dependent on enforcement, which is done through government and through the court system. The tension here is between two conflicting paradigms. On the one hand, the traditional human rights regime, which assigns a major role to states, and, on the other hand, an emerging Internet rights paradigm, in which the role of the state is ideally kept at a minimum. And discussions are now going on regarding a set of norms applicable to the Internet, but also in regard with conserving, for example, different frameworks of intellectual property rights. This is an area, in which the state has traditionally been involved in and has had very strong hand so far.

The Internet has enabled individuals to bypass copyright, but some recent legislative proposals have revealed consistent attempts at using the private sector to control online content, both within and beyond national jurisdiction, which raises a series of concerns as, first, the accountability of the private sector, in the human rights regime, we conceive of it today, and, second, the potential instances of policy laundering, which referred to this changing international regulation by the means of using international treaties.

A third underlying problem is the tension between the Internet as a borderless environment, and degree of variation between states in what concerns,

what is considered lawful or unlawful, and what is acceptable. Here we can think of pornography, copyright, but also political dissent. In this sense, the dual use nature of certain instruments seems to be most problematic. In certain cases, what is deployed for enforcing criminal laws online can also be used for suppressing opposition movements in certain politically sensitive contexts, either directly or indirectly by enhancing surveillance and monitoring. In the UN ambit, I want to point out two recent important developments. The first, one of them is the report of the UN special reporter on freedom expression, which concluded that states have a positive obligation to, and I quote: "Promote and facilitate the enjoyment of the right to freedom of expression and the means necessary to express this right including the Internet", and that the Internet should be a priority on the state agendas around the world.

The other recent event that is worth pointing out in this context, I think, is the landmark resolution passed by the UN human rights council just in July this year on the freedom of expression on the Internet affirming that, and this is a quote: “The same rights that people have offline must be protected online. In particular the freedom of expression, which is applicable regardless of frontier and through any media of one’s choice?” However, this document has a non-binding value, but it

is still showing that important steps forward are taken, and they acknowledge the importance of freedom of expression and more broadly of an online human rights regime that's now developing. Thank you.

DR. S. MALTSEVA: Thank you Roxanna. I want to ask Wolfgang Kleinwaechter to summarise the opinions of our panellists.

PROF. W. KLEINWAECHTER: Okay. Thank you very much, and, first of all, I want to thank the organisers of this workshop to provide the space here for discussion about technology law and human rights. I think it is a very welcome initiative, because if I remember the previous IGFs, we had only a low participation of friends from the Russian Federation, and I take this as a very good signal that, you know, the Russian Federation is a big country, which has a large Internet community, become stronger involved in the discussion of Internet Governance in this multi-stakeholder environment. So, I think this is certainly a positive signal and we can learn from each other, listening to the various arguments and understanding better concepts, very often we're using the same language, but have different meaning behind the same words and this creates some problems sometimes, because that we've misunderstandings, and the beauty of the Internet Governance Forum is that we've here an opportunity to look behind the words, to have individual

discussions with speakers and people from other stakeholder groups as a nation and to find out, you know, what is behind the word, what is the real meaning, this helps us to create understanding. It is difficult to summarise the debate here because we had elaborated individual statements and it is certainly not my task to squeeze out and to say “this was good” and “this was bad”. What I want to do here in my five minutes is to do more of reflection about the relationship in this triangle between technology, law and human rights, and to learn also something from history which is probably useful for the future.

If you go back to the development of technology, and, I think, the first speaker brought us back into the 1940s and 1950s when all this technology started, then you can learn something from previous communication technologies, not only from the 1940s and 50s, but from the 19th century when telegraphy was invented, and then later in the early 20th century when broadcasting was invented. The interesting thing is if you compare this introduction of communication technology with the introduction of the Internet, and put it into the legal discussion, then you see a huge difference. After the invention of the telegraph immediately telecommunication law was adopted on the national level, and the same happened with broadcasting: when broadcasting was invented, immediately the

governments adopted, or the Parliaments adopted a broadcasting law, which regulated very specifically what is allowed, what is not allowed in this new field of technology. And later, then, the governments negotiated treaty based on the national sovereignty, you know, how to organize the cross border flow of information via wireless, and then later via broadcasting. We've a number of conventions, and the ITU is an example of that, because the ITU goes back to 1865, when based on a number of national legislations for telecommunications, then a number of governments agreed, you know, how to organize the transporter telegraph flow, but with the Internet, you know, and this is a surprising thing, this is rather different, because when the Internet was introduced, you know, started with the upper net in the late 60s and in the 70s with the TCP/IP protocol, neither the US nor other country had the idea to introduce an Internet law like a broadcasting law, a telecommunication law, so that it means more or less the Internet developed in a bottom up way in the shadow of governmental regulation, and the regulation of the Internet was done not by the government or Parliament, it was done by the provider and the user of the services themselves. They created, you know, their mechanisms, where they said: "Okay, here we need a certain rule that it functions, and though we saw the emergence of rule making organisations in a bottom up way like what we see today, like the IGF, which makes

standards and protocols for the worldwide web and all this as a self-organised system, and, you know, which was not based on the principle of national sovereignty, because the Internet does not know borders, and though the whole concept of regulating the Internet was totally different from the concept of regulating broadcasting or telecommunication. And this is one of the problems today, because in some countries, some governments have the idea that the Internet is just an extension of telecommunication or of broadcasting and they try to extend this type of legislation to the Internet. You know, which creates now the conflicts with, for instance, in the forthcoming conference in Dubai. The interesting point here with the regulation of the Internet via codes, protocols and things like that. This is really very important to understand the differences, while in the old time it was the law makers, which defined the space for technical innovation, that means when you used, for instance, a frequency outside the broadcasting law, this was illegal. When you used a device outside the licensed devices for broadcasting or telegraphy, which was illegal. That means the law defined which technology could be invented or not, so it means the law maker created the space for the code makers. But nowadays it is the code makers, which create the space for the law makers. The code makers are much faster and, you know, with all codes and protocols like for instance the MP3 protocol for music, they have created a new space,

which now the law makers have to fill, so it means, if you compare the role of the code and the law makers then you see tremendous shift, so the code makers are now sitting in the drivers' seat and the law makers are hiding behind this development and trying to fill the gaps, which are, you know, emerging because the code makers create new spaces, which are very often not regulated by traditional law, which are just regulated by codes, protocols and things like that. I think this is a fundamental change, because all laws are adopted in the past with a bottom up, governmental-controlled process, while the codes are in a top down government-controlled process, while the codes are developed in a bottom up process where everybody can participate, not only the elected law makers in a national Parliament, and also while in Parliament you need 51% to do the legislation. I think law makers, you know, are elected by democratic elections and they have accountability to their people who elect them, but what about the accountability of the code makers? Because code is also made by man, and you can make good code, and you can make bad code. A code can open avenues, but it can also close streets, so I think this is really an issue, which we've to study much more. What is the relationship between law making and code making in a global environment where national borders play only a small role, and I think this leads then immediately to human rights because, you know, one of the freedoms is certainly, you know, what we call today

the freedom of expression, but also the freedom to innovate. While, I said, in the old telecommunication world, this was, you could have innovation only with permission. If you invented something, you needed then a permission to use this. But the Internet is innovation without permission. There is no need to ask. Larry Page did not ask somebody whether it is allowed to start a search engine or not. Mark Zuckerberg did not ask whether it is allowed to start a social network or not. He just did it. And this is also a new challenge too. We're seeing a lot of things where traditional top-down legislation processes, nationally and internationally, are now partly complimented, but also already partly substituted by a the bottom-up process where the policy is made not only by one stakeholder, by a lot of stakeholders. Civil society have a word in this, the private sector, the technical community, and government certainly also needed in this process, and this is a big challenge ahead, and human rights issue is certainly in the centre of it. Roxanna quoted already the famous resolution from the human rights council adopted in July this year, we should be aware that this existing law, which was important for the offline world existing, is important for the online world. And sometimes some people argue, okay, we're in cyber space, we need new laws. We need new human rights or things like that. So, I think, the cyber space is just an extension of our reality, and if we've laws in the real world, then there is no need,

you know, to reinvent everything. We can 99% of the existing laws can be used also for the online world. A crime is a crime. I think, if I steal money in the online world, it is the same crime like in the real world. There is no need to have new cyber security legislation, which would forbid stealing money online, because it is already in the existing criminal law, that stealing money is illegal, and with a lot of other things also, that the existing legislation, both in human rights and also in other fields is very often sufficient enough to deal with all these challenges, so it means I would close here with a certain, I would not say warning, but, you know, I would recommend Parliaments and governments to be very careful, if they move into the field of new legislation for the cyber space, because a lot of the issues, which are, you know, cultural issues, content issues, security issues, property issues or whatever, are already regulated national legislation and international treaties, and there is no need to introduce new legislation. There could be a need, but you should be very, very careful before you start new legislation. What is the subject of the regulation, because very often introduction of legislation has unintended side effects, and sometimes, you know, you want to repair something, but at the end you destroy a mechanism, which works. Thank you.

DR. S. MALTSEVA: Thank you very much. So, we start the session of questions, and general discussion. Please, first of all, questions from our viewers please.

AUDIENCE: Can you hear me? Okay. I'm from Information Technology University. Actually, it is not a question. I just want to add some notes for Andrey's speech. When he means about server installed in some location, and the users in other administration in other location, so that I know that the UN, they release the new law, so if the crime appeared in some country and you have to present this in the manner, any person from other country, they have to bring it back and judge them in their native country. But now they relate the new law, if they are here, the person did the crime in this city, they can immediately judge them in the same country, so I guess the UN will be creating a new law for Internet, when, as Andrey said, if he did something wrong, they have to judge criminal in the country where the court is located. So, I guess this law will be implemented also in virtual world. Thank you.

DR. S. MALTSEVA: Thank you. Andrey, have you some comment?

A. SHCHERBOVICH: Yes, I have a comment. Thank you very much for your attention to my report, and I would like to say that, first, the issue of jurisdiction in cyber space is one of the most difficult issues now in

all legal scope of the Internet Governance issues. So that, I think that, personally, I suppose that we need, as you said, the UN law, the international treaty, which regulates the issues of jurisdiction within the Internet, which we define especially, counter action of cybercrimes. Thank you very much.

DR. S. MALTSEVA: Roxanna, maybe you want to add something, or Mikhail, or anyone wants+ to add to it? No? Another question? Maybe remote question? Question from remote participants? The question to Andrey, how we can protect content in open network?

A. SHCHERBOVICH: Very interesting question. The first, I would like to ask a question back, what is the open network? Internet itself is the open network. There are no closed Internets. In different countries like, maybe, North Korea is closed Internet. They have a computer network but there is no Internet inside, but how to protect information in the open network is, I think, a very simple question and is complicated in the same time. As far as we protecting information offline, we should, maybe, if possible, to arrange application different offline laws. It is one way of protection information in the Internet, and the open networks. The second solution of this is to create and establish a special different rule towards Internet and other networks inside the Internet. The third question is protection of the open information and the Internet by

developing the network communities, on the third level Internet Governance. I don't know, which way is more simple and which way is correct. I think most of them, and the co-ordination between these three decisions would be the best way to protect information in the open network. Thank you very much.

DR. S. MALTSEVA: Thank you, Andrey. And the next question to Roxanna, how do you see the optimal balance between the private and public in the Internet?

R. RADU: Yes. I really wish I had a solution to that. We would be out of here in a couple of minutes and we would start doing something else. I think, this is a question that everybody is actually trying to answer right now. My own insight on it is that we still need a degree of public regulation, but we need to make sure that that doesn't go in directions that have a lot of predictable unintended consequences. At the same time, with the private sector we can notice a series of initiatives like self-organised coalitions that are trying to push forward the accountability for human rights online. Also different types of corporate responsibility for programmes that actually try to increase access to the Internet, and some degree of transparency, which, I think, they are all positive. So, I would just leave it at that, that we see some efforts made in the direction of striking a balance, but it is still developing.

DR. S. MALTSEVA: Thank you Roxanna. Maybe somebody want to add anything?

DR. M. KOMAROV: Yeah. I also would like to add some comments. I think, integration of digital signature, you know, all over the world, not just inside one particular country, would help us to directly define what is private and what is public. For instance, if you know some information is signed by your digital signature, it might show that it is probably your private information, and if it is not, then probably it is a public one, right? Thank you.

DR. S. MALTSEVA: Please your question.

AUDIENCE: My question relates to the Internet black list in Russia. And I'm just wondering, what safeguards are in place to prevent this black list being used to sensor content that's not liked by the government, sensor content that's not liked by corporations as well as to possibly stop and sensor protests both online and offline, and whether any of the Russian panellists foresee this as having an impact on freedom of expression, both online and offline, freedom of association, both online and offline and freedom of peaceful assembly, both online and offline. Thank you.

DR. S. MALTSEVA: Mikhail?

DR. M. KOMAROV: Thank you very much for your question. First of all, I would like to say that actually, you know, this new law and this black list just started to work since 1st November, but anyway we've already got six websites put on the black list, and we've got, I think, more than 3,200 enquiries with the names of some particular websites to the commission. The thing is, as I mentioned, there is no public control, there is no open discussions about particular websites, which should be put on the black list. That's why, I think, it might have special impact, you know, on the freedom of speech and expression. And I also would like to add that since we've got the black list, it is quite hard to, at least, try it now, it is quite hard to control, and to see, which websites are blocked, because we've, you know, this kind of input of information when we just type the name of the website and receive if it is blocked or not, and we don't have the whole list just on the website, which means that it is quite hard to see, which websites are blocked, so some websites might be blocked and we wouldn't know about it until we just typed the name of website, right? And also, as we know, website is blocked by the government organisations, which means that even if we've some protests offline or online we wouldn't do anything until there is a special court dealing with this, you know this problem. So, that's what I would like to say.

A. SHCHERBOVICH: Thank you very much. I would like to add some comments about this problem of the black list. At first, those black lists are effective since just 1st November. So, it is not a lot of days passed since the law become effective. At first, sometimes the law enforcement practice is not much more developed, accordingly this black list is only temporary regulations concerning the efficiency of this black list, and also those black lists are devoted only to prohibition of child pornography, not any other things on the Internet, not other cybercrimes, just this. Specific type of prohibited content could be placed into the black list. Also I would like to add my experience, the practical experience, so that sometimes this black list works not properly. The expert itself, those people who providing the expertise of the website before the prejudicial block, they are not clear, because sometimes leaving inappropriate content on the Internet without taking them down. The third issue that in the Russian legal culture the crime is not good from the ethical point of view. It's historical speciality of Russian nature, so if they have the special form on the website, governmental website, on which we could apply for this prohibit illegal content, but now they will apply for this content in case that some people are damaged by contents of this website. In this case, they will apply. But I think that we need to have some time to see how this black list is working to make some maybe sound decisions on this, and its efficiency, but it is not

the best way to prevent illegal content on the Internet. As for backlisting we know that Russian experience happened that, but we've judicial black list on the extremist websites, which is judicial list not only websites, placed on, but also literature and other, which contents hate speech or discrimination on national or religious nature and they have experience of having this black list in Russia, but it is only judicial black list. Also I would like to conclude about this judicial procedure. Judicial procedure, the trial in Russia is quite long. We've a red tape specific of the Russian trial. It is very simple and very, very short period of time to move this website to another domain and to re-establish this website, so this judicial procedure of prohibiting this site is also still not effective. Thank you.

DR. S. MALTSEVA: Thank you Andrey. Another question? Please.

AUDIENCE: I believe there is a law 436FZ in Russia that requires notices about websites that are not appropriate for children. I'm just wondering what type of technologies are required to implement such a thing where possibly technologies like deep inspection are required, and again the human rights impact. Thank you very much.

DR. M. KOMAROV: Thank you very much for the question. The thing is, when we're talking about

special technological issues of blocking the websites we're talking about, special recognition for analysis of the data on the website of the content, mostly it is implemented right now for the pictures, images, and for the text so it is data recognition on the top operator of, you know, on the country's space, I mean on this level, and after that this operator, or content provider sends notification to special governmental structure saying that, you know, there is inappropriate content probably coming from that side or another one, and it might send official notifications to the local content provider so Internet providers saying that you should block the website or, you know, if it is a country server or, you know, somewhere in the country, if they will block it immediately after the decision on the notification of that top content provider. That's how it works, and technological aspect is just recognition of different pictures and just comparing with some, you know, databases, and with set of some, you know, inappropriate content. So, thank you.

DR. J. MALCOLM: The problem with this is that there is always firstly over-blocking, in other countries where we've had child pornography block lists we've also blocked legitimate content such as sex education sites for teenagers, that sort of thing, so the other problem is that the lack of transparency is inherent to blocking of child sex abuse sites, because the

authorities don't want you to be able to see what is on the list, because they don't want you to be able to go and check out the sex abuse sites, of course, so this is a real problem and the third problem is that it, well, it is not really a problem, but the Internet is designed in such a way that anything that's blocked you can route around and get to, so there are technology, such as Tor, which can be used, and also encrypted VPNs, which can be used to get around these blocks. I think that a more productive venue is to go after this, the production of this material at the source, when we have, you know, crimes committed, we don't go after those, who report the crimes or who disseminate those who use appropriate way to deal with the distribution of illicit material.

PROF. W. KLEINWAECHTER: I think this is a similar lesson Germany learned. We had a discussion in another session today, the terminology legislation, that means that, you know, there is an outcry in society: governments do not understand the Internet, they want to do something, and the easiest thing is blocking and filtering, but this is, indeed, as Jeremy said, this doesn't work. I would not say, it is nonsense, but because it has some intention and probably not the protection of children is the main intention, you've other intentions there, but this is a different story, but the only way, really, is to go for the criminals, who produce the criminal content, and not just to close your eyes or not

let others, you know, block your eyes, this makes no sense. This does not work, and, if you trust the technology, then you know you should learn something from the project in China, they wanted also to block pornography on the Internet and they used a special, you know, picture recognition technology, and so it filtered out websites where you had a lot of, you know, which you could identify as skin, but it was only white skin, so it means while they eliminated all the important sites with white people, all the important sites with black people, you know, were not filtered out because the technology was not able to make this difference between black naked skin and white naked skin, so it means that of you have to, it is a permanent handicap for new technology, technology plays a certain role but you should not trust technology - it can give bad advice.

DR. S. MALTSEVA: Thank you very much. Maybe another question? Yes. But shortly please.

A. SHCHERBOVICH: Thank you. This legislative policy, on which blocking and filtering are based, depends on the content of the Russian segment of the Internet. You know, that there is not everything clear on the Internet. For example, I know that some years ago now it is much better situation is much better, the child pornography was in open access on the major social network in Russia. That's why the blocking and filtering policy is maybe the only and the last way, that could

have positive effect on this, if other measures, for example establishing a legal culture and information culture of users and other things, which could help users to make their behaviour on the Internet appropriate to the laws and to the rules of maybe human moralities as well. Thank you very much.

DR. S. MALTSEVA: Thank you very much. I want to thank all the panellists, the member of our audience and our remote participants for active discussion, and I would like to thank the organisers for this good opportunity to discuss these important problems. Thank you very much.

MOBILE APPLICATIONS AND INTERNET OF SERVICES FOR THE EMPOWERMENT OF DISPLACED PEOPLE AND MIGRANTS

Dr. Svetlana V. Maltseva,
National Research University Higher School of Economics,
Dean of the Faculty of Business Informatics,
Head of the Department of innovations and business in IT.

Dr. Mikhail M. Komarov,
National Research University Higher School of Economics,
Faculty of Business Informatics
Associate professor, Department of innovations and business in IT.

Due to the technological development we faced problem of not implementing new technologies in order to help displaced people and refugees or sometimes we only introduce some basic services. It is necessary to remind about disasters which we unfortunately can't predict and which usually completely change citizens' life. People have to move from their neighborhood to other places (usually) to other countries where they do not know local cultural specification and traditions, local laws and they are not able to assimilate easily.

Technological development already introduced to us global networks – like Internet and GSM, and mobile technologies and devices – like cellphones, tablets and laptops.

The most common and popular solution is our cell phone. For the last 10 years manufacturers brought

cell phones to the new level of development – with cell phone hardware and software called mobile applications which resulted to the fast growth of mobile devices and applications popularity. Mobile devices give us mobility and it is one of the key factors made them popular.

Traditionally, mobility has been divided into four different categories [1]. The first mobility type is terminal mobility, encompassing portable devices that can communicate regardless of location. Personal mobility (or user mobility) is when a user can switch between devices and/or networks and keep her user identity. The third mobility type is session mobility (or continuous user mobility), achieved when keeping media streams or other types of session alive although changing location, device and/or network. Lastly we have service mobility, defined as making services available to a user regardless of terminal, network or other context parameters. Four components are needed to achieve service mobility: a mobile device; network connectivity, supporting mobility; an application providing an interface for user interaction; and a service. Regarding mobile devices, common examples are smartphones and tablets. Developers of mobile applications are focused on spread service-oriented approach all around the world. It tends to the algorithm when applications send data from the mobile devices to the remote server which leads to the big amount of data stored there. Now companies first

think about mobile application and service it would bring than about traditional PC-software and only after that extend software on mobile platforms. Many chief information officers and analysts now bundle mobility with other recent developments like social, cloud and analytics. These four trends are together called SMAC, a term that describes the close association between social, mobile, analytics and cloud [2].

In terms of business opportunities there are already many "e-" services which available through the Internet and via mobile devices (e.g. e-health, e-agriculture, e-commerce, etc.). But the most important from them in our opinion and not from business prospective are services focused on education, law, health and socialization. Mobility brought us within mobile devices and remote servers opened new wide range for the applications and services they provide in these areas. Modern smartphones are able to provide information about you location, frequencies of your text messages you send, average length of your talks etc. All this data helps to personalize applications installed on the smartphone and make service it provides more efficient. Personalization approach within mobility opens wide range for improvement efficiency of applications providing different services. It is also support citizen(consumer)-centricity approach which is commonly used nowadays in different governance areas.

Internet of services and mobile applications for displaced people, migrants and refugees cover the following areas:

- employment;
- skills recognition;
- housing;
- health care;
- finance;
- education;
- youth services;
- vocational training;
- aged care;
- family support.

And there is a group of information services which should provide access to the full range of services mentioned above.

In spite of the fact that services for different groups of migrants have considerable commonality, their effectiveness depends on the ability to adapt them to specific groups and even personalize them. Models for providing information to migrants can become more centered on their problems. Such services may be based on the citizen(consumer)-centricity approach.

This approach today is the basis for business development. Customer-centricity takes customer focus to the new level – and improves loyalty and profit, First

of all it takes into account three aspects: customer lifecycle, customer experience, customer value. The obvious problem for the implementation of this approach is the lack of reliable information on migrants, often due to language problems when filling out questionnaires.

Active use and integration of information from different sources, such as social networks and public data is possible by obtaining the missing information in order to make information services for displaced people more personalized. It is also important to store information about previous calls for displaced people services.

Establishment of standards for the collection and use of information on migrants and displaced people, as well as the principles of the collaborative use of this information would receive and collect information about the life cycle of migrants and displaced people on the basis of which it is possible to improve services and delivery methods. In particular, this can be done on the basis of a single standard for identity of the migrant and displaced person.

Another important aspect is the involvement of e-consultancy for introducing new services. Successful e-consultancy implementation must present the migrant and displaced people consultancy portal as a single enter to its users. Much emphasis should be given to the usability of the services. Qualified advice should cover

all areas, mentioned above and be provided with all available information.

There are few service already introduced for the displaced people. One of them is developed to help displaced people to stay in touch with their relatives and remain being a family even if all the family members are not able to meet each other for some time [3].

There should be multi stakeholder approach introduced in order to define particular set of services and mobile applications which should be developed and provided for free to displaced people and migrants to help them assimilate. There should be discussion about benefits for business being involved in development process – advertisements in applications for free for business to cover expenditures for the development. Or there might be governments introduced as main subsidizers of the development process.

Key considerations for integration/information strategies [4]:

- maximising the potential for joint working and collaboration between state and NGO providers
- different strategies of information provision may be needed for different categories of migrants
- inclusion of a user perspective on information and service provision
- need to prioritise groups who are disadvantaged and to tackle issues and problems of access migrants

information needs differ in some respects from national population – compliance with complex legal requirements

The main conclusion is that both state and business in all the countries should be involved as well as public society and NGOs into the development and implementation process of the Internet of Services and mobile applications for displace people and migrants.

References

1. ITU-T recommendation h.510, mobility and collaboration procedures. mobility for h-series multimedia systems and services. 2012, [Online]. Available: [http://www.itu.int/rec/dologinpub.asp?lang=e&id=T-REC-H.510- 200203-I!!PDF-E&type=items]
2. Pulakkat H., "MobileFirst: IBM asking companies to design mobile applications first, rest later". 2013, [Online]. Available: [http://articles.economictimes.indiatimes.com/2013-02-25/news/37289434_1_mobile-applications-mobile-analytics-mobile-commerce]
3. Charles Hawley, "NGO 2.0: Using the Web to Reunite Refugees". Spiegel. 2009, [Online]. Available:

[http://www.spiegel.de/international/world/ngo-2-0-using-the-web-to-reunite-refugees-a-614590.html]

4. Geralyn McGarry, “Information needs of migrants – outcomes of research into Citizens Information Services”. 2008, [Online]. Available [http://www.dublinpact.ie/new/cCitizens%20Info%20Board-Migrants%20Info%20Needs.pdf]

HUMAN RIGHTS ISSUES ARISING IN CONTEXT OF THE FREE (OPEN) SOFTWARE

Andrey A. Shcherbovich,
National Research University Higher School of Economics,
Lecturer, Department of the constitutional and municipal law

The problems of free (open) software have always been recognized area of interest intellectual property rights and other branches of private law. Such a debate in the public law field is fairly new, but the problem of the proliferation of free software, of course, affects the perspective of the constitutional rights and freedoms of man and citizen.

We consider the use of a free (open) software for the implementation of human rights and freedoms at all three levels of Internet governance. More detail the role of each of these levels in the governance of the Internet in the context of freedom of expression, access to information and other constitutional rights set out in my paper "Freedom of speech on the Internet: the constitutional and legal aspects"[1].

The debate about free software

Free (Open) software, by definition, L. Lessig – this is the program source code is available to everyone. Anyone can download a technology to run the program with open source software. And anyone eager to learn how to operate a separate module of this free technology, can change its code[2]. Despite the fact that this software is beginning to emerge in the early 80-ies of the last century, only in the last decade, its popularity has increased so much that it became able to compete with traditional commercial proprietary software products. Most of this was made possible because of the Internet, has opened a unique opportunity to overcome geographical barriers, the joint work of many programmers from around the world and disseminate the results of such work without spending[3].

V. Slyschenkov and A. Levin noted that supporters of free software is important freedom of distribution of software as such, regarded by them as the value of the same order with the freedom of speech, assembly and other fundamental rights and freedoms. In contrast, open-source software movement this general legal and humanitarian component fades into the background, giving way to the practical considerations

of economic benefits that can be obtained from the work of the open source[4] .

Meanwhile, in the I. Zenina and K. Meshkova noted that free software should be distinguished from the Open Software, software or open source software. The authors of the term "Open Source Software" are Eric Raymond and Bruce Perens. This term is used with the 1998 software is open source software distributed under licenses Creative Commons. Firstly Creative Commons license appeared in 2002 and were designed eponymous social organization Creative Commons. Unlike the GNU GPL Creative Commons licenses allow translation to other languages and the emergence of official translations and adaptations to the laws of other countries.

Creative Commons licenses are more flexible in comparison with the GNU GPL, and let the author as to retain exclusive rights in full or in whole or in part, to abandon such conservation. As a result, not all Creative Commons licenses are free[5].

The Message of the President of the Russian Federation leaders of the participating countries' Group

of Twenty "is proposed to undertake a comprehensive analysis of the prospects for recognition of the right to limit the website of their property rights (partial rejection of them) by way of public statements about the need for the absence of consent and / or the payment of compensation for the use of third-party created Content them for specific purposes. This study is necessary to standardize the existing free license (Creative Commons, etc.) and the adaptation of new models of distribution of content to the requirements of both the Anglo-Saxon and continental law[6].

Of particular note are the activities of international intergovernmental and non-governmental organizations in this field. Activities of a number of them specifically devoted to a free (open) software. The largest of these organizations is the Free Software Foundation - a non-profit organization founded in October 1985 by Richard Stallman to support the free software movement, and in particular, the project GNU.

It is in the communities for professional or cultural interests are added alternative relations, and public opinion is formed. The first example was the community of free programmers, Mr. Richard Stallman

founded in 1984. He set the task to free software from the shackles of copyright and patent law, to "give all users the freedom to redistribute and modify," he developed the program. From thought to announce its operating system of public property Stallman refused, so as not to give any temptation to privatize derivatives. So the idea of «Copyleft» is a special concept, which does not allow using the development of free programmers to create proprietary software[7].

Open content movement is based on principles and values inherent in post-economic thinking, has its own methodology and ideology, a legal right, the driving force and motivation system, as well as ways of organizing production and distribution of digital products specific to the non-hierarchical (net) producing structures.

It may be noted the following principles of open content movement:

1) Knowledge, information, works of art and scientific results in the public domain.

2) Free access to information and knowledge sharing are essential to the development of society and human evolution.

3) Socially useful activities is the result of greater importance than private commercial gain.

4) The collective authorship and collective responsibility - the basis of fair value exchange.

5) Transparency of methods, rules of the organization and the technology used - for the effectiveness of joint activities.

6) The partnership of equals, non-hierarchical, open and free membership in the community - a condition of collective synergy and effectiveness of the team.

7) Commitment to Ethics Network, which is the basis of so-called Netiquette as a set of unwritten rules that govern the rules of behavior in the virtual world[8].

The international level of regulation

Unauthorized copies of software are particularly prevalent in poor countries. The highest percentage of its use in Vietnam, where it is estimated the Business Software Alliance 94 percent of all software used in 2001, was illegally copied. In the article by S. Garfinkel noted that the situation was spread even "in disadvantaged parts of the United States". In Mississippi, 49 percent of the software was contrary to copyright laws.

Such copying is a particular risk for organizations that protect human rights: U.S. companies and the U.S. government are making every effort to make the illegal use of software crime around the world, as in the United States[9].

The International Covenant on Economic, Social and Cultural Rights, in its article, according to which recognizes the right of everyone to enjoy the benefits of scientific progress and its applications. States are called upon to take measures for the preservation, development and diffusion of science and culture. This guarantee, obviously, refers to software that is primarily represents not only the technology, but knowledge in its pure form, the product of human creativity. Contributing to this

particular human right, therefore, also means "liberation" of the software.

Among all human rights, one most relevant to free software is so-called "right to development". It is the third generation of human rights, in recent times has become urgent. It belongs to the category of so-called "human solidarity" (along with the right environment, the world's artistic heritage) that involve social and collective dimension to the implementation of the common good. So the traditional dualistic scheme of "people - the state" is now changing: the human rights of its belonging to the community are met based on the fact that a person belongs to this community. important thing here - this is a concept formulated by the UN human development.

The right to communicate is one of the most talked about civil liberties in the digital world. The claim to the right to communicate is usually followed by a discussion of its aspects, such as the right to privacy, protection of intellectual property, to freedom of expression. As for the free software, there is no doubt that it is the best it's better guarantees the right to

privacy, as well as offering opportunities for creative expression.

The educational value of free software led to the fact that from the very beginning of its use has been linked to the right to education. For many years the bodies of the United Nations, in particular UNESCO, prepared reports on the potential of new technologies for e-learning, in particular, to improve the level of human development. Increased access to education and improving the quality and flexibility of the educational services are among the features of the free software[10].

National (state) level

In Russia at the legislative level, the issue of use of such software does not rise. However, the use of the territory of the Russian Federation of open source development represents a qualitatively new phenomenon in the relationship and the user's software with open source. Note that these solutions are implemented mainly in the form of orders of the Government of the Russian Federation on the development of specific plans for the transition to the use of free (open) software [11] . In the explanatory memorandum to the draft federal law on the

federal budget for 2012 indicated that the project "Modernization and support systems technical support to users of free software for scientific and educational institutions" in 2012, the main results of the implementation are, in particular, for updating training materials to work with the free software used in educational and research institutions, the access to the portal of information and methodological and technical support and distance learning system with the free software from the given parameters of quality of service of the Portal[12].

Senior Research Fellow of the Institute of State and Law, RAS A. Zharova believes that in Russia there are changes in the expansion of the rights of users of computer programs, through the distribution of software, open source (free software), but in this area there are quite a lot of problems. In Russia in 2009, such software has been used extensively in government, ministries, and departments. However, problems still exist because at the moment turnover rights to such software based on the practice of trade.

The main advantage of open source software is the ability to enable a other computer programs. In

addition, intellectual property rights in such programs have no territorial restrictions, as well as many other constraints specific to closed-source software; it allows you to participate in the development of many programmers, which in turn determines the creation of high-end of the program[13].

Free (open) software is used in order to ensure the transparency of public authorities, in particular the electoral field. In accordance with the decision of the CEC of Russia is a translation of individual software components SAS "Elections" for free software if the implementation of information security requirements[14].

In comments to the Federal Law "On Education in the Russian Federation" states that the technological and software tools that are used to operate the official websites of educational institutions on the Internet, to ensure access for users to familiarize themselves with the information posted on the websites of the free and open source software[15].

Thus, the use of a free (open) software can have both positive and negative sides. Positive point - the use of free software is essential in order to ensure the rights

and freedoms of the citizens through the fundamental right to the information age - the right of access to information. However, it should be noted that the use of free (open) software in Russia inadequate legislation on this issue carries some serious risks.

First, the more confidence the software created by well-known manufacturers in particular due judicial guarantees which are protected by user license software in use. These safeguards prescribed in the license agreement related software product, the agreement provides for the mutual responsibility of the user and the manufacturer, clear procedures for settling disputes out of court as well as in court.

Second, in the case of free (open) software sufficient legal guarantees are not clear. In fact, if you have open license legislation has not developed a unified approach to the protection of the rights of holders of source code and derivatives or modified programs. In our case it is important, it is not known who is responsible for the developed software. Therefore, one of the risks is a violation of the law or dereliction of responsibility on the Free (Open) software distributed via the Internet, at instability of judicial practice in the

protection of the rights arising from its use. Thus, the decision of the St. Petersburg City Court explicitly states that "the judicial panel sees no reason for the evaluation as evidence of code content management system, as the system used by the defendant is free software, licensed under the GNU GPL, the code of the legal values for the merits of the dispute"[16]. The very definition of free software is extremely vague and blurry, which is unacceptable for legal safeguards to protect the violated rights. IS Ivanov, commenting on the law to protect children from information harmful to their health and development, points to imperfection "dictionary" of the Law, including uncertainties and, in some cases, ambiguity of the terms used. Thus, there is uncertainty as to whether or not to refer to the information products free software[17].

Third, in the absence of an effective legal framework and effective enforcement under the guise of free (open) software, you can spread malicious software, including embedded in the source code of the program. A special case of this is the digital vandalism, ie intentional damage or contamination of software viruses which may cause real harm to the user. Often with the use of free software is no protection from malicious

programs that could lead to a possible identity theft. Most free software includes viruses deep within the source code, which leads to the fact that the computer is integrated into the global network without the permission of the user and any notifications.

The level of online communities

As for the level of self-regulation (online communities), it is in their best interests and their efforts to extend the free (open) software. Thus, free software can be used to protect and monitor human rights and freedoms. This raises the question of the extent to which the principles and rules underlying Wikipedia, based on the use of open source software to facilitate sharing real-time monitoring can be carried over into the context of human rights? Is there a problem here, a potential clash of cultures? Wiki culture - a reflection to some seemingly utopian idea has universal exchange and cooperation aimed at improving the human condition. Such precedents are historians of ICT, one of which is the idea of HG Wells' the brain of the world "- a global encyclopedia, collecting all available information into a coherent knowledge[18].

By creating this information, ordinary people can produce information products that were previously produced exclusively by professionals in the field of human rights in the process of "co-production". One example is the co-edited articles on human rights, which are placed on Wikipedia. Although the data in these reports may differ from the reports of non-governmental organizations such as Human Rights Watch, the scope of their coverage is comparable and may cause the public interest in human rights issues.

Non-profit tech company Ushahidi provides a platform for the creation of human rights reports by the aggregation of information provided by the public. Originally developed as a map reports of violence in Kenya after the elections in 2008, Ushahidi is now developing a free and open source software for the collection, visualization and interactive mapping of human rights problems in the world. In such cooperation involves ordinary people who are interested in the protection of human rights, and those of the relevant non-governmental organizations is greatly enhanced[19]. Such activity is called crowdsourcing - is the transfer of certain production functions to the general public on the basis of a public offer, not involving an employment

contract. The development of means of communication, especially the Internet and mobile technologies has allowed the commercial project of crowdsourcing be a way to address the humanitarian problems. According to a leading U.S. researcher Dr. C. Shirky, one should speak of fundamental changes in the use of free time. If the age of television most of the time was spent on passive consumption of information today, more and more members of the digital generation are spending time on the production of information and its publication in the public space, where it becomes an issue. Shirky calls such phenomena of "positive deviance" and argues that the Internet allows you to raise "positive bias", changing the culture of leisure time and providing a large range of tools for the implementation of altruistic premises[20].

In conclusion, the Internet is the main venue for the dissemination of a free (open) software, extending both the relevant sites on the web, as well as indirectly. Often, Internet sites contain online services by using the free (open) software. It is therefore necessary to create an adequate legal framework for the free distribution (open) software. To do this, ensure adequate management of the Internet at all three levels -

international, national, and the level of self-regulation. To do so in the future to ensure mainstreaming of a free (open) software in the legal field, both from the point of view of "soft law" and by appropriate binding international treaty on the rights and freedoms on the Internet. It is also possible to adopt a special convention or the optional protocol on the use of free (open) software. It is expected that the international legal basis of relations on the Internet will be substantially updated and expanded during the World Summit on the Information Society in 2015.

National legislation should take into account that the relations connected with a free (open) software, related not only to issues of civil rights, but also directly affect the realization of the right of access to information. Therefore, must be clearly defined in the legislation aspects related to the use of such software. Of course, the law must be a reference to the basic acts of human rights and freedoms, including those adopted at the international level.

References

[1] See: A. Scherbovich Freedom of expression on the Internet: the constitutional and legal aspect. Monograph. – Moscow, 2013.

[2] See L. Lessig, Free Culture / Per. from English. - Moscow: Pragmatics of Culture, 2007.

[3] See: A. Savelyev The free software licenses in the context of the reform of the civil law // Bulletin of civil rights, 2012, No 4.

[4] See: Slyschenkov V., Levin A. Some features of open source software licensing // Journal of Russian law. 2009. No 10. Pp. 85 - 103.

[5] See: Zenin I., Meshkova K. Free license to the Internet // Information Law. , 2011. No 4.

[6] See: Sitdikova R. Providing private, public, and public interests of copyright / researcher. Ed. M. Chelishev. Moscow, 2013.

[7] See Lessig L. Ibid.

[8] See: Kulikova I., Mamchenko A., Meskov V. Open content: methodology of augmenting the public domain in the knowledge society. Dialogue of Cultures - 2010: Science in the knowledge society: a collection of scientific works of the international scientific-practical conference. - St. Petersburg.: Publisher of the St. Petersburg Academy of Management and Economics, 2010.

[9] See: Garfinkel, Simson. The Free-Software Imperative / / Technology Review; Feb 2003, 106, 1; pg. 30.

[10] See: Schiesaro, GianMarco. Free Software and Human Rights. For the International Congress Free Software and the Democratization of Knowledge, Quito, 23 October 2008. [Electronic resource]. URL: http://p2pfoundation.net/Free_Software_and_Human_Rights (date accessed: 07.10.2013).

[11] See: Decree of the Government of the Russian Federation of 17.12.2010 № 2299-r "On approval of the transition plan of the federal executive bodies and agencies of the federal budget on the use of free software in 2011 - 2015".

[12] See Explanatory Note "to the draft Federal Law" On the Federal Budget for 2012 "// LS "Consultant Plus".

[13] See: Zharova, A. Legal description of the use of open source programs // Legal Adviser in the building. 2010. Number 6.

[14] See Decision of the Central Election Commission of Russia of 26.12.2012 N 155/1160-6 "On the Concept of the State Automated System of the Russian Federation "Elections" to 2016 // LS "Consultant Plus".

[15] See: Scientific and practical commentary to the Federal Law "On Education in the Russian Federation" (itemized) / N. Volkov, Y. Dmitriev, O. Eremin, etc. Moscow, 2013.

[16] See: Definition of the St. Petersburg City Court of 22.11.2012 No 33-16052/2012 // LS "Consultant Plus".

[17] See: Ivanov I. Legal protection of children from information harmful to their health and development: advanced scientific and practical commentary // LS "Consultant Plus".

[18] Alston, P. and Gillespie, C. Global Human Rights Monitoring, New Technologies, and the Politics of Information // The European Journal of International Law Vol. 23 no. 4

[19] See Kingston L., Stam K. Online Advocacy: Analysis of Human Rights NGO Websites // Journal of Human Rights Practice, Vol. 5 Number 1, 2013, pp. 75 - 95.

[20] See: Constitutional Law and Policy: Proceedings of the International Conference: Law Faculty of the Moscow State University, 28 - 30 March 2012 / S. Avakyan, D. Agapov, N. Akuev etc.; Ed. By S. Avakyan. Moscow, 2012.

ARTICLES AUTHORS' DETAILS

Maltseva Svetlana

Graduated from the Moscow Institute of Electronics and Mathematics in 1975.

Professor, Doctor of Technical Sciences.

Dean of the Business Informatics faculty of the National Research University Higher School of Economics. Chair of department of Innovations and business in IT sphere. Scientific supervisor of the Masters Programme on Electronic Business. Deputy Director of the Institute of the Information Technologies of HSE.

Member of the International Association ERSIS.

Author of the more than 80 scientific publications.

Chair of the scientific seminar on intellectual management systems, and methodological seminar on Mathematical modeling, numerical methods and program complexes.

Professional interests: Information systems and networks, Databases, e-Business, e-Government, Network Communities.

Komarov Mikhail

Finished PhD studies and finally passed viva in March, 2012; received M.S. in Information technologies and devices with honor in 2010; received B.S. in Information technologies and devices with honor in 2008 from MIEM; received B.A. in Management with honor in 2009 from MIEM.

Received qualification junior engineer-programmer in 2004 from TCF 1840; passed certification exams (Zyxel Communications Corporation (Zyxel Certified System). Certified specialist in wireless sensor networks (NXP semiconductors).

Participated at the different conferences and exhibitions like - CeBIT-2009, CeBIT-2010 (Hannover, Germany), “Networked embedded and control system technologies: European and Russian R&D cooperation - workshop (2009, Milan, Italy), China Hi-Tech Fair (2012, Shenzhen, China).

Awarded with medals and diplomas for the scientific projects; Scholarship from the company Dr. Web (drweb.com) (2009-2010); grant for the scientific project with Fraunhofer IML (Fraunhofer scientific society, Dortmund, Germany); awarded with special President Scholarship for studying abroad in 2010-2011 and studied at the University of Birmingham, UK which also included participation in research projects.

Founder of the Interuniversity Laboratory for Innovative Projects – WiseNet Lab (www.wisenetlab.com); founder of small youth innovative company VEK-21 Ltd., and head of the certified training center (in microelectronics) of the NXP semiconductors in Russia; founder of the All Russian organization "Young Innovative Russia" www.i-innomir.ru which supports talented people in Russia.

Shcherbovich Andrey

Graduated from the National Research University Higher School of Economics, Faculty of Law (Department of International Law) at 2003.

Completed Postgraduate studies at the National Research University – Higher School of Economics (Moscow, Russia); Faculty of Law (Department of Constitutional and Municipal Law) at 2008.

2008 - 2010: affiliated as a project coordinator in the Non-Governmental Organization 'Inter-regional Library Cooperation Centre', working body of the UNESCO Information For All Programme.

2011 - Present: Lecturer, National Research University Higher School of Economics, Faculty of Law (Department of Constitutional and Municipal Law).

Professional Interests: Internet Governance; Human Rights; International Public Law and Procedure; Constitutional Law; Information Law; International Organizations; United Nations; UNESCO; UNESCO Information For All Programme.

Scientific publication

Human Rights on the Internet

Legal Frames and Technological Implications

Volume 2

Editors: S. Maltseva, M. Komarov and A. Shcherbovich

Passed for print: 11.10.2013. Format A5
Type Tines New Roman
Press sheet 5,6
Pressrun 200 copies

National Research University
Higher School of Economics
101000, Moscow, ul. Myasnitskaya, 20