Public Bodies and Officers Using Social Networking Services: Russian Law and Practice

Mikhail Bundin

Lobachevsky State University of Nizhni Novgorod
23, pr. Gagarin, Nizhny Novgorod
603950, Russian Federation
+7 831 462 30 09
mbundin@mail.ru

Aleksei Martynov

Lobachevsky State University of Nizhni Novgorod
23, pr. Gagarin, Nizhny Novgorod
603950, Russian Federation
+7 831 462 30 07
avm@unn.ru

ABSTRACT

Increasing worldwide tendency of using social networking services by public authorities and officials has its consequences for society and individuals. Being created for mostly private intercourse social networks are now often used for other means. The authors suggest several most urgent issues of the undergoing research about legal regulation's prospective for "public" use of social networks, and provide brief analysis of existing Russian law and practice in the sphere, comparing with other countries.

Categories and Subject Descriptors

K.5.2 [Legal Aspects of Computing]: Governmental Issues – Regulation.

General Terms

Legal Aspects

Keywords

E-Government; Social Networking Services; Regulation; Legal Practice; Russia; Public Administration

1. INTRODUCTION

Social networks' on-line services have become one of the main stream in many spheres of economics for last ten years. Some of them have more than 1 billion users through all over the world [1]. Existing social networks provide very wide choice of services from simple exchange of files, documents, messages, music, photos and videos to on-line phones, cloud services and many others. Wide popularity of social networks very quickly have drawn attention of business and state. More companies nowadays are using social networks to promote their sells and for different types of marketing or clients' support services [2]. The concept of Open Government also means to have many ways of communication with the citizens to make government services close to people and improve them [3]. As a result, the existing governmental platforms use analogous to social networks services: on-line messaging, file exchange, clients support services etc. Nevertheless, they are designed for providing public services with specific content and not widely used by individuals for communicating with the world. The government still needs to enlarge its links of communication outside official channels like television, sites of public authorities, newspapers, radio. Using

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICEGOV2014, October 27 - 30 2014, Guimaraes, Portugal
Copyright 2014 ACM 978-1-60558-611-3/14/10...\$15.00
<http://dx.doi.org/10.1145/2691195.2691222>

social networks by public authorities and officials gives them new opportunities like wider audience for promoting public services or pursuing other political or economic means. The number of social networks users is considerably more than those of official platforms. For example, each of the most popular Russian social networks 'Vkontakte' and 'Odnoklassniki' have about 200 millions of registered profiles [4] and Russian basic government services' platform – 'Gosuslugi.ru' at the beginning of 2014 had about 17 million users and 4 million registered profiles [5]. Obviously, individuals prefer to use the same profile to communicate with whatever they want including state organs and officials, feeling even more freely. On the other side, public actors obtain the possibility to promote their decisions, to discuss documents and initiatives with citizens, and as a result make governmental activities more clear and understandable, involving people in E-democracy services. Many new public initiatives in the framework of 'Open Government Platform' from the beginning contained links to most popular Russian social networks, supposing that the existing problems could be discussed on different levels and through different audiences [6]. Brief analysis of governmental official sites shows that in more than 90% of cases they contains links to on-line networking services like 'Twitter', 'Facebook', 'Vkontakte' etc. with official information. It could be a very appropriate moment to ask 'Do they have the right to use social networking services in that way? Where is the limits? Should there be a specific regulation?

2. MAIN KNOT

When speaking about social networking services, the first question is usually whether it is public or private space. [7] From its origin most of social networks provide many on-line services and a part of them are considered as confidential like messages' services or phone services. The main principle is that it is the user registering his profile decide what information he wants to show and share with the world. Most networks' platforms alert users when filling in the profile what part of information will be open and about terms of disclosure of the rest. Some services always remain confidential between users like phone calls and message services. Moreover, the whole architecture of social networks is created for natural persons to share information and for different sorts of social activities through Internet. The situation has greatly changed since. Could the state and its officials acting in the execution of their power to do the same? Actually, the answer – "yes" means that they could act like individuals, but would that be right and could it affect privacy rights?

3. QUESTIONS TO THE GOVERNMENT

Every connection of individual and the State is formal and has a detailed regulation how it should undergo, on what purposes and conditions, the same for the Internet. Russian Federal Law on the Access to Information about State and Municipal organs'

activities contains the definition of official site and a specified description of what it should contain, and who should be its owner (a state, a state organ, local authorities) [8]. Using social networking public authorities and officials go to the place where there are no such rules, mostly those of the social network owners'. Besides all official sites, especially those distributing information that could affect citizens' rights or human rights should be seriously protected and no one guaranteed the same level of protection in case of using on-line services elsewhere. There is also another question of great importance – it is the publication status. Under newest amendments to Russian Law on Information [9] - blogs are regarded as a media and should be registered officially if they have more than 3000 visits per day. The law does not make a distinction between public or private profile owners, so it could be implemented to state organs and officials, who could become Medias.

4. INDIVIDUALS' DOUBTS

Creating a false profile is a quite common case in social networks for different purposes. Surely, in more dramatic situation it could be a case of fraud or other criminal activity. In that situation social network's owner is not liable as he only provides a possibility – a space to create a profile for anybody and not responsible for the content [10]. This should draw to an extremely appropriate question. Could individuals trust public authorities' and official profiles? How can they verify it? For example, "Vkontakte" there is more than 20 of "Vladimir Putin" with different photos of Russian President and with various content from neutral to rather sarcastic [11]. Where is real Mr. Putin in this case? Mr. Medvedev uses "Vkontakte" and has more than 1.7 million readers but also has many "clones". Even if the account of public authority or officer is "real" there is certainly a risk of being hacked as it happened several times with Twitter's accounts and the most recent case with D.Medvedev [12]. In the economics, "black PR" often has the form of false profile created by plotters to form negative image of the company using its name, trademark or other attributes, that can be the same case for public authorities and officials to compromise them [13]. For an individual could be another doubt when using networking services, if he is surveyed by legal authorities and officers – and actually it is so. We can find many examples of sewing people for their publication or activity in social network's profile. Russian Federal Bailiff Service in 2010 recommended bailiffs to use social networks for collecting information about debtors' assets and activities [14]. Thus, individuals to think and evaluate their actions in social networking space and be prudent especially with state organs or officials who use social networks also to investigate or find oppositionists or for another reason not corresponding with individual's interests sometimes secretly through false profiles. We can easily presume that some of us will be not fond of been looking through a profile or sending messages by some public authority or an officer especially acting on their own initiative. It is a question whether they could do it freely, without limits or actually send you a "public spam"?

5. CONCLUSION

Summarizing existing situation on using social networking services by public authorities and officials and brief analysis of actual law and practice several legal issues and remedies are to be suggested:

- 1) Can public authorities and officials use social networking services? For what purposes and where are the limits? Obviously, the general tendency is to enlarge their presence

and actions in social networks, but the fact that they are not private persons and if their actions have legal consequences they should have clear limits according to their purposes, jurisdiction and competence.

- 2) What kind of a profile a public institution or an officer should have in social networks? Probably that could be a specific profile, with an indication of authentication from a social network's owner and a more high level of security than implemented to the other users' profiles. Surely, the profile's content is also can be subject for regulation, what information it should contain and its legal status.
- 3) What remedies an individual has for protection from being looked by public authorities and officials using social networking services? Could he bans such an activity in his profile or restore borders?

The answers to those questions could help public institutions and society to find coherent regulation aiming to establish an adequate balance of interests and protect individuals from unfair 'public' use of social networks' platforms.

6. REFERENCES

- [1] Social Networking Statistics. DOI= <http://www.statisticbrain.com/social-networking-statistics>.
- [2] Social Network Marketing. DOI= <http://www.social-network-marketing.org/>.
- [3] Social Media Metrics for Federal Agencies. DOI= <http://www.howto.gov/social-media/using-social-media-in-government/metrics-for-federal-agencies>.
- [4] Social Networks in the World. DOI= <http://ria.ru/infografika/20130321/928343464.html>.
- [5] Gosuslugi Platform Developing. DOI= http://www.gosuslugi.ru/pgu/cms/news/view/NEWS/000000/00000/archive_news/1467.
- [6] Open Government Platform. DOI= <http://open.gov.ru>.
- [7] Basdevant, A. 2013. Les réseaux sociaux sont-ils des espaces publics? In Manara C. *Réseaux sociaux: 101 questions juridiques, A l'initiative de l'ADIJP*. Ed. Diateino.
- [8] Russian Federal Law on the Access to Information about State and Municipal organs' activities. DOI= <http://www.rg.ru/2009/02/13/dostup-dok.html>.
- [9] Federal Law on Information Amendments. DOI= http://www.consultant.ru/document/cons_doc_LAW_162586/.
- [10] For example, Facebook terms of use. § 16 p. 3. DOI= <https://www.facebook.com/legal/terms>.
- [11] Research request. DOI= <http://vk.com/search>.
- [12] Russian PM's Twitter hacked, posting 'I resign'. DOI= <http://www.bbc.com/news/technology-28786683>.
- [13] Skype's Twitter, Facebook and blog sites compromised by Syrian Electronic Army [Update]. DOI= <http://www.neowin.net/news/official-skype-twitter-account-compromised-by-syrian-electronic-army>.
- [14] Russian Federal Bailiffs Service's Recommendation on using Internet for collecting information about debtors' and their assets. DOI= http://www.consultant.ru/document/cons_doc_LAW_114313/