UDC 37

SECURITY OF PERSONAL DATA IN SOCIAL NETWORKS

A. PETROVSKAYA, V. BOGONENKO
Polotsk State University, Belarus

The article addresses strategies to ensure personal integrity and how to protect civil rights from various offenses. A definition of social networks is presented, various risks and threats to personal user's information are investigated, as in a network domain various attacks are made in order to threaten a private life.

Introduction. Information technology is quite widespread in the modern society. Many people lead "double life": online and offline. Involving users in social networks and making people participate in them is a form of intromission into private life, soul, well-being, or into the field of privacy and personal security. Information systems can be a goal, a method, a way, or a place as well as a mean of committing various offenses.

Therefore, the main purpose of the article is to study features of social networks when ensuring privacy and protection from unlawful acts. It is also important to mention many opportunities presented by social networks to contribute to the improvement of social welfare or can be used to prevent, detect and suppress offenses. The potential value for the study is to propose the setting of limits on social networks.

Threats to personal information on social networks. User's safety (security, confidentiality) has always been an important element when connecting yourself to a computer network, and it is still relevant today when using social networks. Users understand the limits of such confidentiality differently; the discussions about its degree always vary, depending on interest groups and cultural contexts. It is worth showing the scheme of social networks engagement versus real communication engagement. Shortly, a number of participants in online communication can grow by attracting relatives, friends and colleagues. Each of your contacts can join (by adding) communication using any "direct" common connection. Nevertheless, such a "friend" (contact) in a real life will encounter serious "communicative" difficulties when joining communication, that is why such a scheme does not apply in a real life. Nevertheless, users of social networks and their "friends of friends" easily get into closer relationships than it is possible in offline communication. Usually user's information is available to "friends", "friends of friends", "friends of friends of friends", etc. Sometimes user's profiles are completely available online, while in ~~a~~ real life this information is available only to a narrow circle of relatives, neighbors or close friends; exists only in official archives and, of course, is confidential. It can be argued that in social networks everywhere and at any given time there are "message boards" on which information is read out, though in a real life such information is considered private. [1, p. 173]

Social networks have significantly transformed privacy principles. To characterize a person in an offline society means to spend a lot of time, efforts and energy. The characterization of a person in a cyberspace or in social networks takes only few clicks: various aspects of socio-demographic information.

Individuals usually indicate on social networks: physical attributes, family life, education, work experience, hobbies, achievements, awards, daily activities, consumption habits, financial situation, housing category, car owning, travel time and direction, psychological state and character traits, political opinions, the information about relatives, as well as similar information about online "friends". The more information you post about yourself, the more vulnerable you are. Even with all the security measures taken, information leakage is possible.

Just after private information is posted on social networks, it hypothetically becomes publicly available on the Internet, regardless of spatial and language boundaries. The functioning experience of social networks confirms that privacy threats are increasing due to the willingness of most users to share private information (including confidential) online, making it accessible by individual users (user groups), relatives, friends and colleagues. Such behavior may be based on the motivation for self-disclosure (self-presentation) through which confidential information becomes publicly available. Thus, the use of publicly available confidential information in illegal activities is one of the main problems in social networks. Active and deliberate disclosure of confidential information by users themselves is carried out, as a rule, due to the underestimation of threats to their own security. Another aspect of the problem is the "passive" disclosure of confidential information [1, p. 174]

Thus, active and passive disclosure of personal information significantly increases risks of confidentiality in network space. Being so easy to obtain user's personal information in social networks and considering the methods of its use, we can conclude that the effectiveness of fighting such illegal behavior with the help of traditional jurisdictional means, is insufficient. As a result, the significant amount of user's data, including personal information, images, audio and video materials are used by unauthorized people and becomes available for public.

The more information is shared, the more likely it is that someone who is pretending to be a regular user can get someone's personal data by deception, or by downloading illegal software and providing access to restricted sites.

Unauthorized access to user's accounts. Violation of home privacy (unauthorized entry) which occurs in a real life, regardless of other harm, is a criminal offense in accordance to the national legislation of many States. When these States determined the consequences of illegal entry into the digital space, many of them criminalized actions such as unauthorized access to information systems, information resources, and account information. For example, in *the Republic of Belarus*, criminal liability for unauthorized access to computer information occurs under *Art. 349* of the Criminal Code of the Republic of Belarus. Unauthorized access is defined here as unauthorized access to information, stored in a computer system, a network or a storage device, accompanied by a break of owner's security system (unauthorized access to computer information), which entailed the inadvertence, alteration, destruction, blocking of information or malfunctioning of a computer equipment or causing other substantial harms.[2] *The object* of this crime is the procedure of accessing to computer information, *the subject* is computer information.

Since the idea of unauthorized access appeared, a distinction has been established between a regular and a malicious "hacking" of accounts. The usual "hacking" is unauthorized access, which is not followed by damage or illegal use of information. A malicious account "hacking" can be used to commit other crimes, including credit information stealing, stalking of legal owners, fraudulent activities on social networks, gaining competitive advantages, illegal enrichment, threats to public safety and even terrorist activities. At the same time, the consequences of usual hacking of an account and unauthorized access to personal information can often lead to much more serious consequences for users of social networks. Socio-demographic information available to the attackers, personal data, financial and economic information, a specific characteristic of the daily routine and behavior patterns of individuals make them as potential victims of various crimes, since they encourage their tracking, search, and stalking.

How to protect your anonymity in a social space? Anonymity in social networks is the most controversial topic which covers a wide range of legal issues. Human rights organizations insist on the anonymity of users because otherwise the real personal data of users is opened and unhindered, and as a result it may be illegally used by government agencies, corporations, criminals and prankers, which may lead to online censorship and violation of freedom of speech, to mass and targeted surveillance and data collection, to the detriment of civil society interests.

It is not a secret to anyone that today a person spends too much time near the computer. Most often, he or she spends this time on the Internet. Some people work online, but most just spend their time communicating on social networks, such as: VKontakte, Odnoklassniki, Viber, Instagram, Twitter, etc. For example, citizens of the Republic of Belarus spend on average about 8 minutes 47 seconds on YouTube per day (the days when a user visits the site are considered), the average number of unique page views per user is 5.07. The second place goes to the search: google.com - 7 minutes 42 seconds and 9.54 pages per visit, the third - the site of the social network "VKontakte" with the results of 10 minutes 4 seconds and 4.69 pages. Yandex.by, Mail.ru, Tut.by, Onliner.by, Google.by, OK.ru and Wikipedia.org are on the top 10.[3]

Spending such a huge amount of time on social networks, it is impossible not to leave at least some personal information about yourself online. By uploading photos posting on pages, or sending instant messages or e-mails we automatically leave information about ourselves that can be used against us. In this case, this information is personal data for which the protection is necessary. Many do not take it seriously, and then regret it. After all, if personal information is in the hands of tracers, this can lead to bad consequences. For example, the most common is blackmail. Having obtained confidential information about you, tracers immediately try to get money out of the person (money, various values, etc.). Of course, no one wants his or her personal information be disclosed, whether it is correspondence, or a photo, or something else. In such cases, people are forced to pay.

There are many ways you can gain unauthorized access to an account. Therefore, all information will be obtained by attackers. Of course, it is better not to allow this, having previously taken care of the protection of personal data.

Having studied this problem, we can give 5 basic recommendations for protecting personal data in social networks:

1. You should not run dubious programs sent from a stranger, or even from a friend (as his or her page can be hacked).
2. Try not to open doubtful messages from any unknown sender, and even more so do not click on links that may be contained in these messages, as these may be malicious links. For example, you follow the link, and your computer automatically downloads a program that has been created and placed there by intruders.

3. Check all downloaded files with antivirus software, as special malicious programs can be placed in them. For example, a program that sends information from your computer to any other ones, mainly to an attacker's computer.

4. When entering the password, carefully check whether it is a real main page of a social network (there are sites that are designed to receive information by entering the "password" and "login" lines), for example, the main page Vkontakte - https: //vk.com. If, highlighting the link, we see an extra letter, or at least some changes, for example - https://vkontakte.com, it usually means that this site was created by attackers.

5. When using someone else's computer, you should remember that all the information you enter (passwords, correspondence, etc.) can be duplicated in special text documents, not to mention the fact that you need to check the password box, and even more so, you need to leave the social networks where you are logged in.

Fulfilling all 5 points will improve the protection of *personal data* in social networks. But the most important thing is to think everything carefully before sending a message, a document, a photo to someone, even if they are in a private message. Suffice to say that one can hack almost any page on any social network and all this data will easily be used by *cybercriminals*. Therefore, you should take all actions the *Internet seriously*, because every action you perform on the World Wide Web can be used against you.

To protect from external Internet threats, you must use host-level intrusion prevention systems (HIPS). A well-developed security policy, and the use of other information protection softwares, as well as HIPS, provides a very high level of security performance. When all measures are taken into account, one can get protection of personal data from almost all types of malicious softwares. Otherwise, you can suffer huge damages which can damage your reputation.[4]

Conclusion. Social networks have become a part of human life. Today there exist all sort of opportunities for cooperation, communication, and information retrieval. One should not forget about the danger of such opportunities. Protecting personal information is always important. In addition to conscious and active disclosure of the information, there is a possibility of passive disclosure of information, which much more often exists in the functioning of social networks. Social networks are subjects to various violations which are associated with a violation of user's privacy, as well as his or her anonymity. Social networks is everything that is associated with pre-existing and new methods for their implementation. There are various ways to ensure the integrity of personal information in social networks. Depending on national law, such decisions unite authors in two approaches: anonymity of users and real identification of users. In fact, both approaches accompany dealer services. The situation is further complicated by differences in socio-traditional customs and behaviors of users and political and legal concepts of the States where users live. It makes impossible to create transnational rules. The international initiative here depends on advocacy. Only practice can answer whether such a protection should be based on user's anonymity or require universal real abilities.

REFERENCES

1. Донг, Ш., Ли Кс. Защита личной пользовательской информации в социальных сетях: дилеммы правоохранительной деятельности практики Китая // Юридическая наука и правоохранительная практика № 4. – 2015. Режим доступа: https://cyberleninka.ru/article/n/zaschita-lichnoy-polzovatelskoy-informatsii-v-sotsialnyh-setyah-dilemmy-pravoohranitelnoy-praktiki-kitaya. – Дата доступа: 24.01.2020.
2. Уголовный Кодекс Республики Беларусь: принят Палатой представителей 2 июня 1999 г.: одобр. Советом Респ. 24 июня 1999 г.: текст Кодекса с изменениями и дополнениями на 11 ноября 2019 г. № 253-З– Минск: Амалфея, 2019. – 304 с.
3. Dev.by [Электронный ресурс] / Digital 2019: тренды использования интернета, соцсетей, мобильных платформ, электронной торговли по Беларуси. – 2019. – Режим доступа: https://dev.by/news/digital-2019-belarus. – Дата доступа: 24.01.2020.
4. Чернобаев, С.В. Защита персональных данных в социальных сетях // Международный студенческий научный вестник № 2. – 2016. Режим доступа: http://www.eduherald.ru/ru/article/view?id=14322. – Дата доступа: 24.01.2020.