USERFOCUS - TOOL FOR CRIMINALITY CONTROL OF SOCIAL NETWORKS AT BOTH THE LOCAL AND INTERNATIONAL LEVEL

Stanislav Šišulák

Academy of Police Force in Bratislava, Sklabinská 1, 831 06 Bratislava, Slovak Republic

E-mails: stanislav.sisulak@minv.sk

Abstract. There are many benefits, but also risks related to using the social networks. Among the benefits of social networking belong an easy way to be kept in touch, sharing news, photos, videos and statuses with friends, colleagues, but also meeting new people with similar interests. The risks include, in particular, loss of privacy, misuse of shared records, abuse of personal data, unknown real identity of social network members, and even addiction on social networking.The paper focuses the need to invent a complex tool of prevention in the field of controling the criminality in particular the users of social networks. In the papers is introduced a proposals how to develop a specific prevention tool called "Userfocus". Further, there are described techniques to implement this tool into the social networks. The work comprises a research (questionnaire survey) aimed at users of social networks and their understanding of prevention in social networks. The results showed that the communication (interaction) among social network users is a main reason to actively use those services, loss of privacy is the most negative aspect of social networking, the perceiving of users related to the fight against anti-social networks is mostly negative, they strongly agree with the necessity to apply preventive methods focusing the user of social networks and consider the developing the preventive techniques and their application by competent authorities in prevention of crime on social network.

Keywords: social network infiltration, Userfocus, profile, intervention, anonymity, security

Reference to this paper should be made as follows: Šišulák, S. 2017. Userfocus - tool for criminality control of social networks at both the local and international level, *Entrepreneurship and Sustainability Issues* 5(2): 297-314. http://doi.org/10.9770/jesi.2017.5.2(10)

JEL Classifications: K14, C88

1. Introduction

Crime prevention is a very important tool in fighting the crime and other antisocial activities. The better chosen form of prevention results in more effective fight against crime. Prevention tools, in general, must reflect the evolution of society and use the opportunities that generate generational progress, whether at technical, social or economic level. This times offer a great deal of information, which the individual, as a cell of the society, is not able to process in a quality, to provide him with adequate value. It was therefore necessary to develop a system capable to store the information in sufficient quality and to create useful databases, which concentrate the quantity and can classify it, so the user, respectively the end user of information is able to quickly and easily find what he need. Today it can be said it is not so important to know the information, but it is important to know where to find this information. Large amount of easily available information allows the communication between the users, who seek this information. Over the last decade, the technologies that were primarily developed for communication among people, they are well advanced to create a more global structure, which can be called a social network.

Now, we do not talk explicitly about online social networks, but the complex structure of the relationships that are created without limitations of space and social disparities, that are removed due to the possibilities of new technologies. The virtual reality is a phenomenon of the 21st century and we cannot say that the growing trend of Internet and online social networks in particular, will shortly have decreasing trend. But also the freedom in communication and diffusion of technology into everyday life has its pitfalls and dangers that without the proper protection of the individuals themselves will grow. The use of new technologies often brings situations that directly threaten the safety and even the lives, health and property of individuals. In connection with the development of new communication tools, particularly via social networks, there comes to the fore the question whether the global nature of this phenomenon cannot be used as a mean of targeted crime prevention. Crime prevention is a very specific discipline, which must respond to the new criminal demonstrations, not only applying the theoretical knowledge, but mainly by practical fighting the crime in its origin environment. This fact may be extended also to another fact that crime prevention can be primarily effective, respectively more effective, even in an environment that does not evoke the individuals themselves to be in a criminal environment outwards. This means that the prevention of crime against the individual types of crime can be more effective if its tools would be used appropriately and properly in an environment, in which the individual feels safe and well, and therefore is not under the pressure of disturbing circumstances, e.g. under the impacts of crime on his live.

1.1. Crime prevention

The society as a whole needs a set of specific rules to ensure its smooth operation and fulfillment of elementary needs of its individual parts, especially people themselves, for its function. However, it is obvious that in such a complex social structure of human society, which is influenced by customs, traditions, religion and other accepted opinions, arise situations which result in the violation of not only the established moral and ethical rules, but also in illegal activity, enshrined in various legal norms.

Therefore it is necessary to adapt the social relations by legal regulations and other generally binding regulations which violation is followed by sanctions or criminal penalties. Such a procedure of authorized bodies is important and irreplaceable from the society protection point of view, but broadly speaking, it is necessary to look at the possibility of preventing the illegal activity, in particular its most serious forms. In this case we are talking about the crime prevention or about the prevention of illegal activity.

Crime prevention can be generally defined as a set of social and legislative measures and strategies aimed at reducing the risk of illegal activity and their potential harmful effects on society and individuals. The crime prevention, in general, involves a complex structure of institutions and processes, involving not only the state authorities, but also non-governmental organizations and individuals. The aim of this process is particularly the positive impact on the individual subjects of society not to commit the illegal activities and vice versa to avoid becoming a victim of anti-social activities.

The crime prevention can be approached in terms of different models and typologies. There should be noted especially the most basic hierarchy that includes:

Primary prevention – it identifies the assumptions, causes and conditions in the social environment that creates the opportunities for committing the illegal activities and further defines procedures that are effective to be used in coping with the adverse events. It operates globally and generally.

Secondary prevention − it includes early identification of potential offenders on the basis of certain characteristics and predispositions in risk groups and aims at acting in the way to have positive impact on the social environment to avoid the harmful consequences to the various subjects.

Tertiary prevention – it has an influence on the subjects that have previously illegal committed and works toward preventing a repetition of the criminal phenomena in the social environment, in principle.

Such a division of the types of prevention can be applied globally. However, the prevention structure includes much wider typology that is developing on the basis of the development of the society through social, legislative and economic perspective. Using a more specific division we come to the clear conclusion that the use of primary, secondary and tertiary prevention features can be implemented in various subsystems of different typologies of crime prevention in a horizontal plane. Nowadays, we can define several ways to approach prevention alone, each one has its irreplaceable role in prevention policy and the particular approaches are interrelated. Thus, we can define:

Criminal Justice Crime Prevention – specific kind of prevention, directly joining the crime prevention and repression into the system of crime control by the competent authorities. This type of prevention is active only after engaging in illegal activity and its mission is to eliminate another potential committing a crime not only by the offender himself, but also by others, uninvolved actors in the criminal legal process. In particular, it is the use of such tools, which use alone deter the committing of illegal activity, particularly the type of punishment, its fair imposition, efficiency and speed of the criminal process, causality between the illegal act accomplishment and subsequent integration into the society, etc. This is a very difficult process of creating such tools to be sufficiently effective, but legislative negotiable. Such prevention is directly dependent on legal norms of particular states and their national criminal law policy.

Situational crime prevention − form of prevention used in a social environment in specific situation or event. Generally, it is focused on the prevention of anti-social activities in the risk environment, but it is important to exploit its full potential, namely the development of a preventive strategy in a particular environment, which includes the specific environment and subjects whose behavior is not as much variable as at the global level. Situational prevention is very good to use, e.g. in the environment of the Internet, social networks, but also in the communities.

Crime Prevention Through Environmental Design − this type of prevention is very similar to situational prevention, but it is focused on the fact that crime is not distributed linearly throughout the territory of a country, respectively globally, but there are so called "hot-spots", where there is an assumption of increased incidence of criminal phenomena, based on social, economic, political and other influences. It is therefore necessary to focus not only on the positive influence of subjects in this area to commit illegal activities, but also on the preventive action in places that may have the potential to become such "hot spots" in the future.

Community and Social Crime Prevention − based on the premise that crime affects many social, legislative, economic factors that can be influenced by effective prevention tools to reduce the risk of committing crime and its prevention. We are talking mainly about direct changes of the poor social and economic factors in risk groups as well as educational and legislative activities. The most effective prevention strategies in this area are strategies targeted at specific disadvantaged or vulnerable community subjects. A prerequisite of such prevention is to strengthen the community through specific programs and selected services provided in order to raise awareness of the risks and consequences of the illegal activity and even the risk reduction in relation to potential offenders.

Individual systems for the prevention of crime and their very specific subsystems include comprehensive preventive strategies and measures that result in prevention projects and programs, which are followed by the specific prevention activities and actions, and imply different prevention tools and techniques of crime control. If we want to create an effective comprehensive or partial tool for crime prevention, it is necessary to create a strategy with a clear focus and vision that is long-lasting and has a definite aim.

Advanced technologies of communication, implemented in cyberspace are specific phenomena and therefore prevention in this space must reflect these specificities and to establish its direct activity on the overall condition

of the structure and in the cyberspace. It is therefore necessary not only to develop strategies and measures, but also specific tools used for immediate control of crime, fighting it and development of educational solutions to users. However, it is not necessary to use a global instrument, but rather specific, situational applications, aimed at a specific group of users or individuals themselves. In this group of preventive tools, respectively prevention activities, the Userfocus can be included as a tool for direct performance of prevention in the cyberspace, particularly in the social networks environment. At the same time, it can be subsumed under the situational crime prevention, operating in a certain specific location (social network) in real time.

1.2 Crime prevention in cyberspace

Crime prevention, in general, is not only prevention of the commission of illegal activities, but it is rather large methodical, empirical and training institute, which is based on knowledge, experience and practice, implementing the appropriate tools and techniques in the global and critical environments. The cyberspace can be assigned to those critical environments. It is a virtual space that is far beyond the possibilities of the real "material world", with its specific processes. Based on the past experience and trends, there is no doubt that it is possible to commit a number of illegal activities in this environment, which amount and intensity increases in proportion to the expansion of this environment among the users and also with the innovation and the development of advanced communication and information technologies. It is therefore important to highlight not only the reasons, the conditions and the possibility of committing the illegal activities in the cyberspace, but mainly the ways to act on users preventively, using the appropriately selected tools and techniques.

In a virtual environment, it is necessary to approach the prevention in correlation with the specificities it brings. However, it is important that the procedures of the individual competent authorities are based on a validated methodology from available information sources verified in practice. Here comes the necessity of aggregating the knowledge and assessment of their applicability in the real prevention, applied to users in cyberspace. Definition of prevention, or its individual tools, is an important milestone in the effective fight against illegal activities of individuals or groups. The logical consequence of these facts is the created summary of knowledge published in the field of crime prevention in cyberspace.

Smyth (2005) in her essay "Crime prevention and community safety: From realspace to cyberspace" introduced the need to prevent crime in cyberspace, noting applicability of preventive tools used in real space to be applied also in the virtual one. She gives an emphasis on so-called "community policing", public supervision of cyberspace in co-operation with the competent authorities, recalling also the legal or application problems, posed by the implementation of preventive tools in the virtual space.

According to Sadhukhan et al. (2015), the attacks in the cyberspace pay attention mainly due to the risk of violation of privacy or confidential security of sensitive information, as well as financial transactions, but does not explicitly need to focus on such mechanisms and crime prevention methods, which are generated from the perspective of the attacker. It considers the protection of cyberspace to be an obstacle rather than an opportunity for the offenders of illegal activity.

Work of Somer, Hallaq and Watson (2016) presented at the "European Conference on Information Warfare and Security" is aimed at understanding the strategic importance of cyberspace and its use in many areas of life. Those are logically also under attack of individuals or groups, who act illegally in this environment. It also shows a way of using areas outside the cyberspace, in crime prevention, right in the risk environment. According to the authors, using the mapping of attackers procedures and monitoring of methods of attack, it is possible to properly understand the actions of offenders and then to target individual tools and techniques on the prevention of specific issues.

Akatyev and James (2015) expressed the need to focus not only on the definition of "cyber war" and the corresponding response of the competent authorities of the state of crime in the virtual environment, but especially on "cyber peacekeeping", thus keeping the "peace" conditions in cyberspace, endeavoring to define this term as the possibility of preventing illegal activity in this area.

"Hacking and Cyber Crimes: A Preventive Guide" created by Moustafa et al. (2013), defined the trends in web and network security in the context of detecting and preventing crime in cyberspace. This study analyses the important types of cybercrime such as hacking, Denial of Service (DoS), the spread of computer viruses, digital piracy, credit card fraud, spam, phishing, spoofing and social engineering, and proposes different countermeasures tools in terms of prevention and repression.

For prevention of crime in cyberspace, Sekgwathe and Talib (2011) expressed the need to detect and protect the cyberspace against the cyber terrorism, outlining the basic procedures of offenders in the attacks, as well as their motivation. The paper published in "Communications in Computer and Information Science", is aimed at provision of a broad overview of the challenges, facing the world of cybercrime and the problems faced by law enforcement agencies, and experts in the field of information and communication technologies security. But they also point to the benefits that can be obtained from the international community and of course from the public and private sector in the prevention, detection and investigation of cybercrime.

Looking at the above mentioned publications, there is a clear need in the definition of crime prevention in the cyberspace as well as creating the theoretical basis for new prevention tools, which must be the result of real experience of users and competent authorities. The possibilities that virtual reality offers, must not only be observed and described, but also applied in the fight against the anti-social activities.

A real and useful tool in this way is the Userfocus. The aim of this paper is not only to describe it precisely and theoretically, but also to give real examples of its use in cyberspace, particularly in the area of social networks. Social networks represent a special environment that requires a specific approach, due to the number and variety of users, and in particular the application parts related to social networks, high complexity. It is an interconnected environment with strong social background that reacts to any change or implementation of new technology to their specific way.

1.3. Userfocus

The crime prevention tools, as was mentioned above, must, in a global context of the illegal activity, directly reflect the real possibilities for the perpetrating of such activity, and thereby create tools that can effectively prevent the manifestation of the illegality elements. Following this idea, we cannot overlook the fact, that in present technologically advanced period, the concept of a crime prevention tool has a new dimension. The use of virtual tools and social networks for communication, as the prevention techniques of the primary and secondary prevention, is an important factor for the realization of power and possibilities of the virtual environment, in the context of preventing anti-social activities. So, if we focus on the socially most important environments in the virtual environment, i.e. social networks, we can talk about new opportunities for prevention, using an environment of social networks and its original tools, that were developed for the purpose of communication and social interaction among users and virtual environment, including its capabilities. In terms of these facts, there is a question, how it is possible to create a framework of measures in the sphere of crime prevention, which would comprehensively cover the use of social networks and virtual environments for instant communication of user, completed with prevention tools. This issue cannot be considered as the standard issue of development of new preventive techniques and tools, because in this perception the non-standard tools application should be considered, that do not interfere with the prevention of crime in general. In terms of the development of crime, in particular the development of illegal activities in the virtual environment and via information and communication technologies, it is necessary to establish a concept that would reflect this development, which practically will be

capable to effectively fight against criminal manifestations in such environment. However, with crime on social networks, such as computer and information criminality, the certain patterns of reflection depending on the virtual environment are changing.

This is not a fundamental proposition of criminology, which states that every object is reflected to the surrounding environment and to other objects and this process is mutual for all objects in the environment (Krajnik, 2005). It is rather complexity and demandingness, which should be considered in documenting the incident site, which a social network can undoubtedly be. However, we cannot state the conclusion that the term "prevention technique" is the only best solution for the future, since the environment and signs of anti-social activities are proportionally developed, too. Therefore, it is necessary to start with a preventive tool that embraces a wide range of users and is able to individualize prevention to a particular user at the same time. Userfocus concept or focus on specific user includes a preventive tool and the related preventive techniques, which implies using adequate possibilities of social networks and other virtual resources for the prevention of anti-social activities at each user individually. It means maximizing the potential use of preventive tool, following the development of individual techniques for a particular user or group of users with the same or similar characteristics.

Based on this definition the Userfocus may specified and precisely defined as a crime prevention tool, used to control, operata and evaluate the prevention techniques in the environment of social networks. The Userfocus as such can be seen in the two spectra, in the narrower and wider, while the narrower is talking about strictly focusing preventive techniques for a specific user (i.e. "superuserfocus") and wider is talking about a set of preventive techniques that are used on social networks in preventing the commission of anti-social activities of their users. Social network, in this definition, is specified as an object of the Userfocus, the tool of prevention, and the user as a specified subject. Their properties can not be generalized, because in cyberspace, there are so many types of social networks with different focus and different users, who behave differently in the specific social networks, even if it is the user, who use multiple social networks. Therefore, we can talk about these two major components of the Userfocus concept, the special subject and object, which are specific just for this prevention tool.

Looking at the complexity of the structure and the amount of data contained in the social network, it is required to view the issue of prevention in this area as a complex problem that requires well-defined processes and structures, which output is a comprehensive tool, serving fulfilling the needs for harmonization of preventive practices in the social networks environment. In comparison of the above mentioned and the concept of Userfocus itself, we can say that this preventive instrument fulfills the conditions imposed on it. It is necessary to take this issue as a dynamic problem, constantly evolving, along with the content, and application part of the social networks.

The socialization of the society via social networks creates wide virtual space that is attended by a large number of people who have exchanged a myriad of information. Right this activity is the main source for the formation of anti-social activities and dissemination of sophisticated and latent criminality, while the possibilities and abilities of users are increasing in proportion to the development of new technologies that the social networks reflect. It is the result of the efforts of social networks to maintain their potential on market with information and information channels, while this market, deployed mainly in virtual space, we can consider for the strongest and most widely used in this context.

Userfocus as such should be based on some basic facts and on realistic tools that on social networks work for holding users interest. In particular, those are the marketing and media tools, application parts of social networks and interest groups that bring together a large number of users. Userfocus can be called prevention tool that uses specific techniques, which are developed in accordance to the interests and needs. Their number cannot be determined, and their development should reflect the development of information technology and in particular the development of the social networks. The basic principles of Userfocus, as a means of prevention, are:

1. *Focus on a specific user and user groups* – the principle of Userfocus is precisely to develop such prevention techniques to reach a large number of users, while they must be individually designed for an individual or a group with the same or similar characteristics. Another important aspect of the Userfocus is the real focus on prevention in general, but also specifically in the environment with the great potential of major crime situations.

2. *Use of existing effective tools for social networks* – the interest of users of social networks and their tools is enormously large, which can be seen mainly on the fact that the need to be on one of the social networks and actively establish contacts on it, it is considered to be a standard today. Today's mobile platforms that are a common part of our lives (e.g. mobile phones, tablets, personal computers, laptops and even watches) practically enforce, with its predefined application, often to use the social networking services, because the applications are included directly in the software. This fact is well understood by the groups that need to promote their products or services and therefore have developed a tool, applying which they can successfully reach a large number of users, with minimal effort and investments. In order to effectively preventatively operate in a particular environment, it is necessary to use tools which are effective in that environment. By the modifications of particular effective tools for the prevention needs, respectively Userfocus itself, we can obtain user-friendly and interesting techniques that can reach a large number of users and achieve real results.

3. *Direct communications with users* – Userfocus should provide preventive techniques consisting of direct application part and the users of the social networks would be motivated to reflect on the primary objective of the specific preventive techniques, by using this part. It means to develop a user interesting and effective preventive tools, using which the user would better understand the prevention principle, create a positive relation to the prevention of anti-social activities, and would be motivated enough to be able to continue to act preventively to his surroundings. It is important to note that such prevention should be focused on a particular type of anti-social activities, and embedded in a specific environment, what is a designation of the Userfocus, as a mean of prevention.

4. *Complexity, individuality and flexibility of preventive techniques* – The most important aspect of Userfocus is the individuality of its techniques. This individuality is mainly based on the diversification of social networking environment and its users. This fact means that it is not possible to develop a general preventive tool that would effectively cover such a large amount of users and still really operate against anti-social activities. However, all techniques that Userfocus contains represent a basis for building a comprehensive system that has its own rules and aspects, focusing mainly on primary and secondary prevention. It is also important that the Userfocus reflects the development of modern technology and the progress of social networks in the sphere of new tools and application parts development.

5. *Evaluation of the real results* – if we would like to develop a real functioning tool of crime prevention, it must be developed in terms that this tool is measurable and evaluable. The Userfocus must therefore be designed so that the results can be statistically evaluated. It means not only to evaluate how many users were affected by each technology, but particularly the evaluation of the state and development of anti-social activities in the environment, or between users, where each technique was focused.

The purpose of these principles is to develop a new preventive tool that can operate effectively in a wide range of users, while also develop such preventive techniques, which are actually measurable. To properly define the Userfocus, it is important to build a comprehensive system for defining users into specific categories and then develop a system of individual preventive techniques. It is also necessary to point out the key features of the *Userfocus in the whole context of prevention* – the Userfocus is not just a method of crime prevention in the environment of social networks, but primarily an effective preventive tool in the global aspects to perpetrate crimes as such. It should be mentioned, however, that this type of crime, which includes various illegal activity manifestations, has its own specificities that characterize it (Metenko et al., 2004).

1.4. Target groups

The Userfocus as a preventive tool should pre-eminently be focused on the user. We cannot look at this issue globally and develop techniques that will try to cover a wide variety of users, while their outcome will be vaguely measurable, due to the wide scope. It is therefore necessary to diversify the target group of prevention in this case to the categories, related to the certain characteristics of the individual users. The ideal application of the Userfocus is specifically focusing the individual users and setting such techniques that reflect the interests, personality and environment of users, not only from virtual, but also real life. In this case, we can talk about technically very difficult process that must be developed based on the experiences and techniques results, focusing the user groups. These can be divided to the following categories:

Groups divided by the age − one of most elementar divisions, which is based on the age structure of users and divide them into the groups according to age. The Userfocus on social networks can create very specific age division, even down to the individual user age and this way to direct the specific technique for different age groups. Age is an important factor in developing preventive techniques, as understanding and perception of prevention is commonly based on the user age. Therefore the age as a factor in the use of preventive techniques cannot be ignored, even when it is used for other classifications. It is also an important factor in determining the priorities in the prevention as such, respectively in determining the appropriate techniques based on risk factors and risk groups. Age also determines the number and frequency of preventive techniques applications within the Userfocus. With regards to social networks, this means that the most important groups - children and young people - in terms of prevention must receive much more real prevention through social networks. Also the bullying via the information and communication technologies has its origins in the opportunities that present time provides mainly for young people (Tomkova, 2016).

Groups divided by the gender − gender is also an essential factor in the division of users to groups. In real context, we should come out from the fact that one group, the women, are more vulnerable, regarding the violent crime in particular. In terms of gender, there can be distinguished only two groups, while we should not forget the importance of distinguishing the prevention among women and men.

Groups divided by the interests − in the context of social networks we can talk about groups of people, where the Userfocus preventive techniques can be applied most effectively. Since in the area of social networks, there are so many users with different interests, it logically resulted in their associating in this environment and creation of groups, where they can share experiences, communicate with other users, etc. The division of interest to subgroups and setting the preventive techniques of the Userfocus, depending on the risks and problems of particular interests logically result in a very effective technique that can directly intervene and operate specifically on a large number of users with real results. However, the groups of interests should be classified to risky and less risky. Risky interest groups are particularly extremist groups, groups that promote criminal or other antisocial activities and so-called group "on the sharp", whose activity is not illegal, but live in an environment in which the users can create values and opinions that can affect certain user groups inappropriately.

Groups divided according to the social environment − in the Userfocus, it is the most demanding division / classification of users, since the social networks are not yet able to define the real social status and environment of their users. However, the development of technology for social networks does not exclude the possibility that the users would eventually be divided into social groups in the future. For the Userfocus tool it means it will have particularly qualitatively better application of its preventive techniques, too. Various social groups need different preventive techniques and different prevention scope. Diversification of social user groups is particularly important in relation to individual types of crime and techniques that can operate against perpetrading the anti-social activities. This division should not be perceived as casting of individual users, but there must be comprehensively applied the potential, which in future will bring social networking tools for more effective prevention in this environment.

Group divided by the quantity of contacts − this division is very specific and reflects the socialization of users on social networks, in particular. The division based on the quantity of contacts is aimed mainly at preventing the perpetration of crime and other antisocial activities on social networks, because there moves a large number of perpetrators of criminal frauds and other criminal and illegal acts in this environment, who use suggestive techniques to accomplished their deeds, where just a user of social networks is suffered. A large number of contacts and their very high anonymity can cause many problems to the users of social networks and therefore is important very sophistically to apply the social networks tools for effective prevention, measurable particularly in terms the users begin to consider adding the suspicious or unknown people to their contacts.

Groups divided by the education − education is a measurable feature, but does not reflect the factual level of education and intelligence of individual users. Therefore, in this case is difficult to develop preventive techniques to effectively engage a wider range of users. But even education need not to be excluded in the dividing / classification of users, because it is a factor that affects the prevention and user communication settings applying various techniques.

Individual approach − in this case, we are not talking about the division of the users, but about the so-called perfect Userfocus, which techniques are created based on information from real and virtual life of individuals, who use the social networks. The basic principle of individual approach in the Userfocus is such a development of preventive techniques and outputs of these techniques that reflect the individual personality of each user. This process is a long-term goal of the Userfocus and is currently technologically very difficult. But this may be real in a short time, especially due to the progress of technology and social networking. In principle, the individual approach can be understood, in the context of existing social networking tools, as the establishment of properties by the above-mentioned and other classifications and harmonized into a complex system. However, it should be also mentioned that with the development of social networks also an individual approach to the user will be developed. It will result in the development of more effective preventive techniques of the Userfocus.

In the context of the Userfocus and dividing the users into groups, it should be noted that this issue is complex and should be therefore understood in relation to each other. This is an important point that should not be missed. The individual users must be classified into several groups, which clearly facilitate the individual approach to individual and creating of less wide broad preventive tools. The effectiveness of prevention on social networks must be measurable, while its outcomes will help to develop the preventive techniques and the Userfocus itself.

1.5. Userfocus techniques

In the context of the Userfocus preventive tool, it must be pointed out that without the adequate techniques serving for direct interaction with social network users there would be no reason to create any preventive tool. Therefore, it is necessary to create groups, types of techniques that should have specific outcomes and would create the concept of prevention in the social networks themselves. It is also necessary to develop techniques reflecting innovation on social networks and focusing the continuous progress of tools and applications used by social networks. The Userfocus techniques can be divided, based tools and applications used by social networks, as follows:

Techniques using interest groups − in this case we are talking mainly about the integration of prevention of certain interest to the community of people who join together and communicate based on the interest. If we define the risks associated with certain interests, you need to create a counterpart to the risk, which means creating, respectively of infiltration in which we wish to act preventively. When you create an interest group that focuses on crime prevention (especially, but also globally), it must be ensured clarity of thought, clarity of content, focus on active users and especially the motivation of association in the present group. Groups and pages on social networks are the best starting point for Userfocus as such and we can work on them with a wide range, and social

networking tools. In practical terms, we can say that the creation of such a group, and in particular properly managed can be achieved by grouping a large number of users with a specific interest, which can be defined as specific, and based on their presence in the group to act preventively using the techniques of Userfocus. Creating posts, status, add videos, creating applications and other social networking tools, in combination with appropriate techniques of Userfocus, can clearly define its objectives and measurable results clearly recorded.

T*echniques using the social networking tools* − following the group of previous techniques, it can be stated that the user integration itself is not enough to create a successful prevention tool. It is necessary to use all the tools that social networks offer and to implement the Userfocus techniques to these tools. Those are particularly the tools that are subjected to the interaction of users and also the possibility of the impact of these tools on the user, mainly the application parts of social networks, sites and groups. It should also be noted that the Userfocus must essentially reflect and react to new technological tools of social networks and to implement them in their techniques. Social networking tools, in this case, fulfill the role of direct contact and interaction with the user, while cannot be only a simple flow of information without feedback, but the effect of prevention using these tools with real results. Communication of users, with directly specified information on the prevention, means mutual interaction and creation of an environment, where the users think about the purpose of preventive techniques and especially about the fight against crime and other antisocial activities issues. Social networks tools provide options that are inherently unique, while the effect of prevention, respectively Userfocus, is practising every time the user logs on to the social network site. However, the main problem of this issue is the suitability and appropriateness of developing the preventive techniques and their application itself.

The use of marketing tools (Perina, 2011) − the massive expansion of social networking among common users logically resulted in entering the marketing and media tools into this environment and the creation of a specific market with advertising and promotional tools. These tools are used to distribute information about products and services, and that is why they must have their indisputable place in the context of the Userfocus. In this case we are not talking about the development of the Userfocus tools themselves, but rather about their faster and more efficient distribution among common users. Marketing tools have very strong distribution opportunities, but their use requires having expertise in marketing and funding. Therefore, it is necessary to use all available information and practical experience in advertising and marketing, to minimize costs for the Userfocus techniques distribution.

Gamification (Guštafík, 2016) − this term refers to the use games in non-game environments. Gamification is a powerful way of positive influencing especially the children and youth, and especially in their natural environment, which is a social network undoubtedly. This method of interectation with users is a suitable technique, where it is necessary to recognize the need to create application part with the form and content to be preventive tool. The game focusing the preventive action should be easily manageable, logical, undemanding and motivating, whereby it is necessary to use a social networks application environment. This method is the most effective to distribute the game with prevention character to a wide range of users. Game, respectively playing the interactive games, can also be one of the factors to focus on a particular user. In case of the Userfocus, there should be created several types of games, which in the global aspects will cover more user groups and individuals and will have a higher success rate. Looking at the use of Gamification, e.g. in education, we can conclude that this method of Userfocus preventive techniques can have a very large percentage, as is understandable and acceptable for all types of users of social networks.

Special profiles − in this case we are talking mainly about using one of the tools of social networking and its assigning among the special techniques of the Userfocus. In practical terms it is to create the user – preventer profile, who, based on his active influence on the users, creates a preventive effect. In particular, he comments the events on the social network, communicates with users, adds the positive contributions and statuses - in terms of crime prevention, etc. The main feature of the special profile is mainly the credibility, because also via the Userfocus, there should be pointed out the screening of their own contacts with specialized profiles, while the

specialized profiles can, based on their transparency and meaningfulness, assist in this sphere. Also in terms of the Userfocus, we can talk about the variety of specialized profiles, focusing on the different groups of users or other means of prevention, respectively prevention of various types of crime.

Talking about the concept of preventive techniques of the Userfocus, it is important to note that their use is not confined to use only one technique, the best and most effective way to achieve the desired goals and the result applying the Userfocus, is to use a combination of different techniques, while focusing on a specific group. It maximizes the achievement of the desired goal, which may be really measurable, when using the highly specific techniques of the Userfocus. It should be noted that the various techniques of the Userfocus are developed together with the social networking tools. The producers of these techniques must have a certain degree of creativity in developing these techniques and their implementation into the social networks. Thus, the Userfocus can occupy a very clear and important role in the prevention within this modern and virtual environment such as the social networks, after the development of appropriate techniques.

1.6. Particular examples of Userfocus techniques

The basic precondition of the Userfocus as a preventive tool is the reality of its techniques development, aimed at defining the appropriate roles and procedures in the implementation of individual processes in the environment of social networks. In the broad context of social networking tools, there can be developed a large number of techniques of the Userfocus. There are introduced some of them:

Positive massaging – The principle of this technique is to create a profile on the social network in order to act preventively to other users, while the task of the user responsible for this profile is to act in direct manner, thus creating the blogs, commenting, messaging and using the communications tools of the social network. In this case, we can also talk about the possibility of forming a structured system of users, aimed at different groups of users, respectively focused on individual prevention thematic blogs (drugs, cyberbullying, pornography, grooming, etc.). In the real context it comes to writing positive comments about individual products of the social networks (photos, statuses, etc.), that are capable of acting illegaly, respectively antisocially, due to their nature and the way of presenting. Responsible user, therefore, despite the hateful commentary, writes positive comments to manage the already existing problem. This means, it is not a cyber hate or a hate in the Internet environment, that represents a set of illegal speeches directed against ethnic, racial, sexual or religious groups and their members, using the information and communication technologies (Bihariová, 2012). Applying this technique, the user may not only act preventively. Of course, there are statuses, comments and messages of a preventive nature, pointing out or reffering the address of certain issues in the environment of social networks, with the relationship to avoidance of antisocial activity. Positive massaging is a technique directly confronted with the users and therefore it is very important to develop methodologies and a user base that knows the social networking tools and can respond to changes in a virtual environment. In case of this Userfocus technique we are talking about the primary prevention.

Individual intervention − In case of this Userfocus technique we are talking about direct interaction with individual users. This technique focuses on secondary prevention, i.e. on subjects where there is an increased risk of becoming perpetrators or victims of crime. There are applied the tools of social networks, directly related to preventive action on the subject. Individual prevention is divided into several stages, the first of which is monitoring the environment and searching for the target entity. In the second phase is collected and evaluated information about the subject and in the third phase comes to the intervention itself, in the form of targeted advertising, targeted positive massaging and other targeted techniques of the Userfocus. The aim of this method is to search for users and user groups at risk and act not only preventively on those users, but also to obtain information and practical knowledge on the structure of social networks, new forms of crime, etc. Individual intervention is a complex technique of the Userfocus that uses also other techniques of the Userfocus effectively to achieve the objectives of this preventive tool.

Anonymbox − The aim of this technique is to create an anonymous mailbox, into which you can virtually "send / insert" the message, while the principle of this technique is collecting messages with character of illegal activity. In real terms, it is a mailbox, where users can send / insert their experience, expertise and knowledge on the illegal activity on social networks. After sending / inserting such message to the mailbox, this one is evaluated and subsequently, there are adopted measures to prevent possible illegal activity.

Following the examples of techniques of the Userfocus, it is important to note that the operators of social networks themselves create the conditions for the implementation of preventive tools in virtual environments and has also implement measures of preventive and repressive character to prevent illegal activity in this environment. But still remains the question, whether such influence of the social networks on the user is adequate and in terms of further development of social networks sufficient.

1.7. Implementation of the Userfocus into the environment of social networks

The social networks are complex environments with a wide range of users who create their content and also determine the technological and social development to a large extent. In such difficult conditions, it is important to create a plan under which it is possible to implement the Userfocus as a preventive technology in this environment and to set its techniques at the same time, to effectively meet the desired goal – really positively act in the sphere of prevention of anti-social activities, especially the crime activities. The plan of implementation is a process that can be defined in several points:

Defining the objectives (target group, crime type) − First of all, it is necessary to define, as by any preventive tools, the aim which the Userfocus should meet. As mentioned above, Userfocus is specifically aimed at a certain group of users and also we can state, to achieve the greatest efficiency, Userfocus must in any case of prevention be focused on a specific type of crime or anti-social activities. If Userfocus is used as a preventive tool on social networks, we can talk about the so-called setting the Userfocus "campaign", that covers all the important techniques to achieve the desired goal. It must also be remembered, that it is necessary to define realistic goals that are achievable by the Userfocus. This part of the Userfocus implementation process in an environment of social networks is the most difficult and is based not only on theoretical knowledge and technological possibilities of social networks, but mainly on practical experience related to using the social networks tools from other spheres.

Creating a "campaign" of the Userfocus and determination of appropriate techniques − In the second step, it is necessary to create a "campaign", so a summary of the techniques and processes that will be used for preventive action on the different groups of users or on individual users. The campaign also includes a timetable and the time range, during which the prevention authority through a campaign will positively influence the users of the social networks. Ultimately, we can talk about the Userfocus "campaign" as the its manifestation outwards, while this includes all the necessary techniques, which have their application schedule and are used specifically for a certain type of anti-social activities and the specific group of users or individuals.

Launch of the "campaign" – Under this term we can understand not only the actual launch of the Userfocus campaign in an environment of social networks, but also the subsequent guidance of techniques and implementation of other Userfocus techniques according the course of the campaign itself. This means that the Userfocus campaign is not strictly intended for the only use of defined techniques, but reflects the development of the campaign and using other techniques makes the preventive action more efficient.

Collecting the results − The most important part of the Userfocus implementation process to the social networks environment is a real capability to measure the campaign results. This means, in particular, monitoring the Userfocus campaign course and recording the results. In principle, it is related mainly to the number of users

affected by individual techniques, the interaction of users with technology, feedback to developed techniques as well as the interest of users of each technology from the time aspect - frequency of interactions, application of techniques developed, with regard to the application environment, etc.

Evaluation of the "campaign" – In the last step in the implementation process is important to evaluate the campaign and also the success of individual Userfocus techniques. Meeting the goal must be measured in absolute terms, while the effectiveness of the Userfocus, as a tool, can be compared with more databases containing statistical data, such as statistics on the perpetration of various types of crime. Also the Userfocus techniques efficiency can bring their more practical use as well as definition of the range of their use and their actual improvement according to the obtained practical experience. The campaign as well as the Userfocus itself must be based on the exact approach and its evaluation is decisive for the further development of this tool. Within the campaign evaluation, there should be mentioned that it depends on the objective specified, as well as on the course of the campaign itself. Even the results must provide explicit conclusions on the success of the campaign.

In connection with the implementation of the Userfocus as a tool of prevention in the environment of social networks, it should be noted that the reality of this process determines also the classification of the Userfocus among the tools of prevention in general terms. The success in this case is defined in particular by the specific environment in which Userfocus operates and narrow specification of techniques used. The particular campaigns of the Userfocus can have diverse objectives defined and can have the multi-level form, that allow defining the milestones in each campaign. Here we should mention also the fact that the globalization of the objective of the Userfocus may result in less efficiency of techniques and campaigns set, and hence demanding real fulfilment of the desired objectives.

2. Experiment and results

When defining the Userfocus, it was necessary to find, how the users themselves perceive the antisocial activity on social networks, as well as the prevention and avoidance of such activities by the competent authorities. The survey was evaluated by completing the survey form by 82 users of social networks. The users, respectively responders, responded five questions. There should be noted especially the relevant facts related to the need of implementation of the Userfocus techniques in this environment. The survey was disseminated via Facebook social network and the responders were only the users of the Facebook social network (random selection).

This approach was chosen purposefully, because this social network is in terms of its tools, options and social interaction most developed and complex. It must also be remembered that Facebook is globally the largest social network. That means that it concentrates a very large number of users. From this fact follow the consequences in the form of a higher rate of incidence related to anti-social activities and the occurrence of new, mostly latent and highly specific forms of such activity, notably because of the nature of the social network and activities of its users.

In particular, the aim of the work was to establish the current view of users of social networks to approach of the competent authorities in the prevention of anti-social activities in this environment, but also to extract the real user experience with crime on social networks. A specificity of the methodology was the fact that the survey was not directly aimed at a particular group of users of social networks, but focused a very broad group of respondents, while the only limitation was the language of the survey - Slovak.

When choosing the right method, it was needed to manage the specificities of the social networks in conjunction with real threats and the consequent possibility of using a preventive tool that would be directly applicable in this specific area. It was therefore necessary to determine the current state of empirical knowledge of the users and then to compare that experience with the proposed techniques of the Userfocus prevention tool. In the end, however, it is not sufficient to draw stark conclusion about the necessity of setting up a specific prevention

mechanism, but in particular to propose the specific procedures to reach this state, in comparation with previous findings of other authors who have solved this issue. It should be also noted that the aim of work was also to document the current mood of users in the field of prevention and follow-up usage of the survey results for the purposes of other related research and studies.

Question survey focused on five important factors. First, it was necessary to find out for what reason the users of the social networks actively use their services. The graph on Fig. 1 shows, that majority of respondents considered the greatest benefit of social networks in the opportunity to communicate with friends and find quickly updated information. It can be therefore stated that the responders use the social networks in particular because their high social interaction (43%) and information profitability (39%).
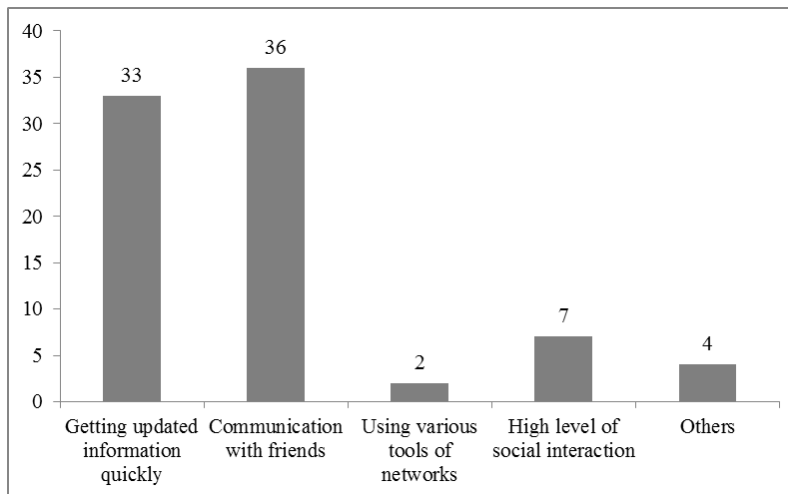

Figure 1. Greatest benefits of social network specified by the responders
Source: Author – realised survey

In the next question of the survey, which results are shown in a graph in Fig. 2, responders expressed the opinion related to the identification of the most negative aspect of social networking. According to users responds, the biggest problem of social networks is the loss of privacy (35%). However, it should be noted, that social networks provide tools that can prevent the leakage of private information.
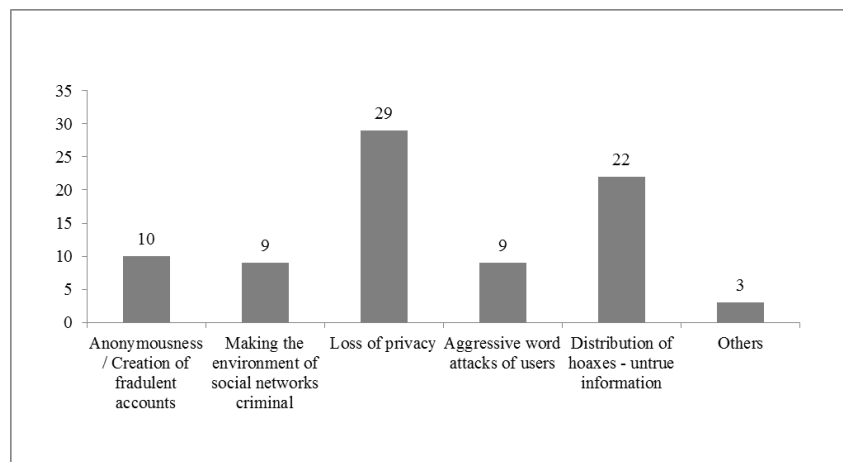

Figure 2. Most negative aspect of the social networks specified by the responders
Source: Author – realised survey

The users of social networks could also to express how they perceive the fight against anti-social activities on social networks. In the graph in Fig. 3 are shown the results, which are divided into two categories - the measures taken by the provider of a social network and measures taken by the competent authorities. The results shown, that the responders evaluated the fight against the negative effects as inadequate (49% / 55%).
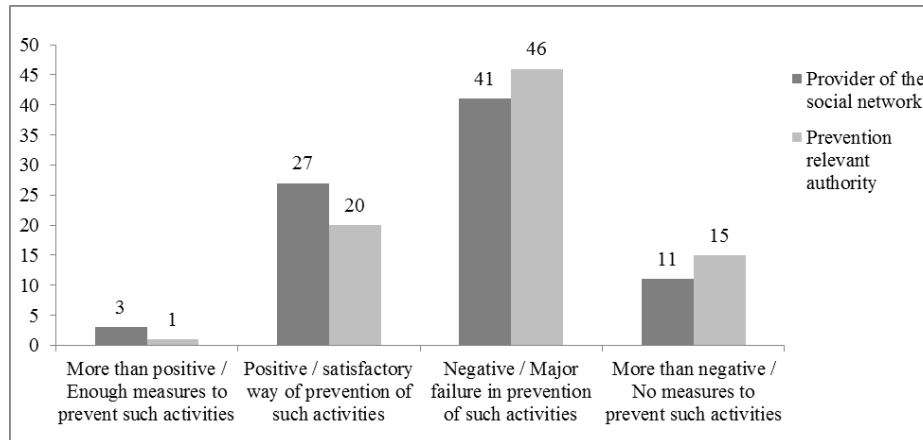

Figure 3. The perception of the fight against the negative effects on social networks
Source: Author – realised survey

An important part of the survey was the question, whether the users of social networks have met with any form of prevention on social networks. As many as 51 respondents (62.2% of respondents) have not met any form of prevention on social networks. That question was accompanied by an open question, while as the forms of prevention, with which users of social networks met, they assigned in particular the measures taken by the social network provider – blocking the inappropriate content, blocking the fraudulent accounts, etc. They also introduced the efforts of the provider of a social network to develop some form of alerts related to security risks, in connection with the creation of passwords, their entering, etc. The graph in Fig. 4 shows the users' opinion on the fact whether is necessary to apply preventive methods focusing the users of social networks. The users were further asked to explain their answers. The most important finding coming from the answers was the fact that the users (64%) perceive the prevention as needed and necessary to prevent the perpetration of anti-social activities and even more effective than repression measures taken by the competent authorities.
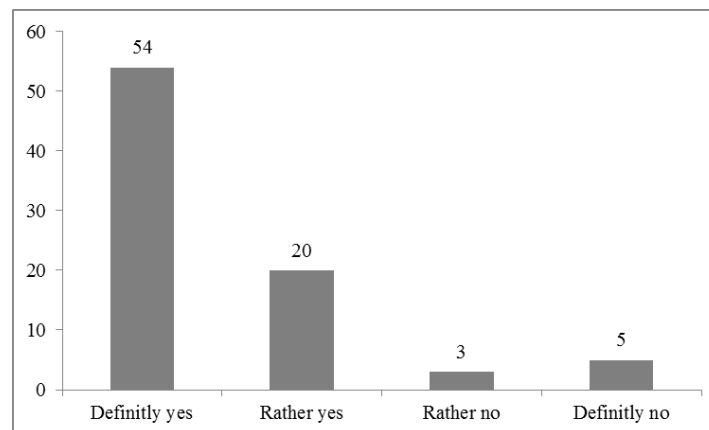

Figure 4. The necessity to apply preventive methods on social networks
Source: Author – realised survey

At the end of the survey, the users of the social networks, was asked to express their opinion on the action of the competent authorities in relation to the prevention of crime on social networks (graph on Fig. 5).Almost 30% of respoders expressed their will to develop preventive techniques to prevent negative activities in the social networks environment. The will to apply the crime prevention measures on social networks, directly in risky groups in the schools expressed 27% of responders.
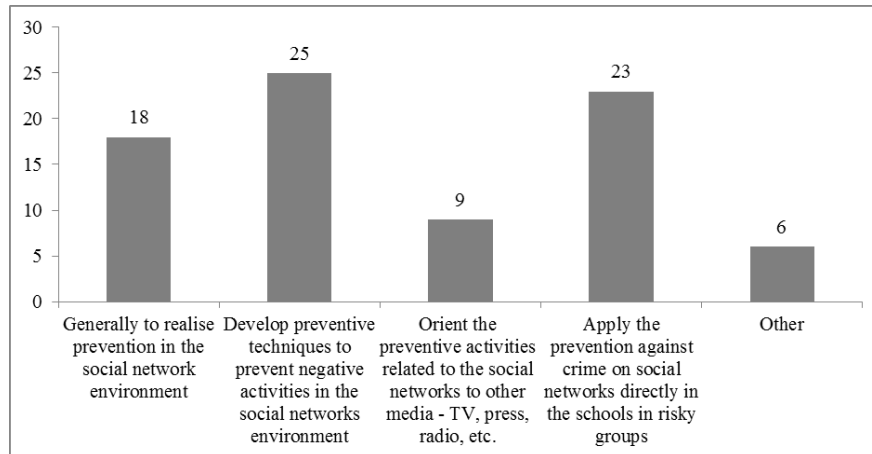

Figure 5. The perception of the fight against the negative effects on social networks
Source: Author – realised survey

3. Discussion

A clearly defined role and objective of determining the concept of Userfocus in this study was to provide a basic framework and outline of preventive instrument, which due to its specification extends the boundaries beyond the conventional method of prevention in the cyberspace. The aim of this process was not only todescribe the theoretical structure of the instrument itself but also to bring real-life examples of its use in practice, what is the most important part of the experiment. As part of work was to identify and reflect the experience of social networks users with the prevention of crime in this area as well as their perception of the prevention tools that are used on social networks. It is clearly evident that the majority of the respondents sample considered the action of the competent authorities or the actual operator of social network in the field of prevention to be insufficient, and this fact showed that it is more than necessary to seek and develop new prevention tools that effectively and comprehensively cover such diverse environment of social networks. Looking at the structure, meaning and purpose of Userfocus, it can be stated that it is one of the appropriate tools to be implemented in this environment, however, the results results achieved with this tool, even they are really measurable, can be detected during its real application.

In comparison with already published studies in the field of crime prevention in cyberspace, it can be stated that there raises a real need for the creation of these prevention tools and techniques which are applicable in the real environment of social networks, respectively in cyberspace and are intended to reduce or eliminate straight antisocial activity, educate users and act on potential offenders or persons who have committed the offenses. It is crucial to apply the knowledge from this area to create a kind of "knowledge and experience network", serving for exchange of experience and finding new opportunities in the field of crime prevention, not only in the cyberspace. In case of Userfocus, we are talking about a particular specification of a useful tool, while it can be concluded that using the way of closer specification of crime problems in cyberspace is necessary to work also in the future, to create specific measures to fight the crime and other antisocial activities.

Conclusions

Social network and its tools provide options that are used in all areas of our lives. From a sociological perspective, the social network is a social structure, which consists of a system of social actors (individuals, organizations, etc.) and dynamic relations among actors (Wasserman, Faust, 1994). Prevention of crime and other antisocial activities have recently been inflected as an urgent need, and thus it is necessary to apply this need in a virtual environment, too. Userfocus as a prevention tool is an example of how to develop an efficient tool to optimally use the possibilities offered by social networks. It can reflect the real state of anti-social activities and also crush it. To apply the Userfocus and its techniques is needed to mention that its feasibility and applicability depends on many factors, which are based on the environment of social networks themselves. The success of this tool depends also on creativity and technological security of preventive authority, who should apply the Userfocus to social networking environment. Userfocus offers opportunities to be grasped and used for the benefit of preventing the anti-social activities, and the based on the techniques determining the Userfocus, effectively operate against such action. Implementation of Userfocus in an environment of social networks is a long process. The first step is to establish an authority responsible for searching the antisocial activity on social networks, while inferring also real consequences, not only in terms of prevention, using the Userfocus tool and techniques, but also in the form of direct intervention against disturbed social relations.

References

Akatyev, N., James, J.I. 2015. Cyber peacekeeping. *In Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, LNICST 157, pp. 126–139. https://doi.org/10.1007/978-3-319-25512-5_10

Bihariová, I. 2012. *Cyber hate – nenávisť na internete*. [Cyber hate - hate on Internet]. Available on the Internet
http://www.beznenavisti.sk/wp-content/themes/beznenavisti/podklady-a-materialy/Cyberhate-Nenavist-na-internete.pdf

Brantingham, P.J., Faust, F.L. 1976. A conceptual model of crime prevention. *Crime and Delinquency*, 22(3): 290.

Clancey, G. 2014. *Thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy*. University of Sydney – Faculty of Law.

Guštafík P. 2016. *Gamifikácia vo vzdelávaní: čo to je, ako na ňu, a prečo o ňu usilovať*? [Gamification in education: what it is how to on it, and why seeking it?]. Available on the Internet: http://www.pdcs.sk/sk/blog/gamification-vo-vzdelavani.html

Krejčí, V. 2010. *Kyberšikana*. [Cyberbullying]. Available on the Internet: http://cms.e-bezpeci.cz/content/view/14/39/lang,czech/

Meteňko, J. et al. 2004. *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality* [Investigative techniques and sophisticated options to control crime]. Bratislava: Akadémia Policajného zboru.

Moustafa, A., Al-Shomrani, M.M., Al-Marghirani, A., Al-Rababah, A.A. 2013. Hacking and cyber crimes: A preventive guide. *Journal of Engineering and Applied Sciences*, Vol. 8 (7), pp. 225-229.

Perina, T. 2011. *Sociálne siete a ich využitie v marketingu*. [Social networks and their use in marketing]. Trenčín: Vysoká škola manažmentu v Trenčíne.

Sadhukhan, K., Mallari, R.A., Yadav, T. 2015. Cyber Attack Thread: A control-flow based approach to deconstruct and mitigate cyber threats, *International Conference on Computing and Network Communications*, CoCoNet 2015, art. no. 7411183, pp. 170-178.

Sekgwathe, V., Talib, M. 2011. Cyber crime detection and protection: Third world still to cope-up. 2011. *Communications in Computer and Information Science*, 171 CCIS, pp. 171-181.

Somer, T., Hallaq, B., Watson, T. 2016. Utilising journey mapping and crime scripting to combat cyber crime. *Proceedings of the European Conference on Information Warfare and Security* (ECCWS), January 2016, pp. 276-281.

Smyth, S. M. 2005. *Crime prevention and community safety: From realspace to cyberspace (MR07360)*. ProQuest Central; ProQuest Dissertations & Theses A&I.

Šišulák, S., Šalmík, M. 2013. Cyberbullying ako forma zneužitia sociálnych sietí na internete [Cyberbullying as a form of abuse of social networking on the internet], *Policajná teória a prax*. 21(4), pp. 112-123.

Tomková, J. 2016. *Adolescenti a negatívne zážitky na internete. Kyberšikanovanie*. [Adolescents and negative experiences on the internet. Cyberbullying]. Available on the Internet: http://www.prevenciasikanovania.sk/

Vnouček, P. 2010. Facebookový vrah má doživotí. Sociální síť sklízí kritiku [The Facebook murderer has life. Social network reaps criticism], *Týden*. Available on the Interne: http://www.tyden.cz/rubriky/media/internet/facebookovy-vrah-ma-dozivoti-socialni-sit-sklizi-kritiku_161662.html

Wasserman, S., Faust, K. 1994. *Social Network Analysis: Methods and Applications*. Cambridge: Cambridge University Press.

Stanislav ŠIŠULÁK is the Vice-Rector for Informatisation and Co-ordination with Police Practice, Academy of Police Force in Bratislava, Slovak Republic. He is responsible for management of the Academy and for co-operation with the practice of the Police Force in Slovakia.Research interests: internet security, cyber security, crime prevention.
ORCID ID: orcid.org/ 0000-0003-4727-9582