Społeczeństwo, polityka, stosunki międzynarodowe
Keywords: organised crime; cybercrime; cyberstalking; cyberbullying; crime prevention; witness protection

Abstract: Cyberstalking has become a new form of crime and deviant behaviour. The authors research the problem of cyberstalking and intimidation via the Internet in details. These concepts are used interchangeably because all forms of stalking are threatening or have the purpose of distressing the victim (victim stress exhaustion). The authors tried to draw attention and show the interconnection between the social danger of cyberstalking and the violation of private life boundaries. The consequences of such interference can cause the significant harm to man interests, material harm; threaten the physical and mental health of a person. The authors in this article draw attention to the activities of people who use the Internet to threaten (intimidate) others. The phenomenon of cyberstalking constitutes one of the main aims of the analysis because it includes a rather large area of behavior performance (starting with the expression of threats to the theft of personal data). The main question of this research is simple: what makes an intelligent and law-abiding person in the offline world (outside the Internet), take part in anti-social or criminal activities online? The basic reason is the fact that the combination of technological and social factors encourages people to participate in crime or antisocial acts, such as incitement to violence against other people. The originality of the study is that the authors analyzed the public danger of cyberstalking and the consequences of privacy infringement by the negative impact on a person through the Internet. Authors highlight trends and developments, and give recommendations on how cyberstalking prevention matters can be improved.

1. Introduction

Socially interactive technology (e.g., mobile phone text messaging, social network sites like Facebook and Twitter, etc.) has permanently changed our communication landscape, allowing users to interact electronically with one another in a way that was once inconceivable – being physically absent yet instantaneously accessible and connected (Marganski 2017). Cybercrime, software piracy, illegal downloading, hacking, and cyber bullying among others have all become part of our daily lives (Udris 2016).

Since the advent of the Internet two main forms of stalking have been distinguished: traditional stalking and cyberstalking. According to Miller (2012) traditional stalking is a subcategory of generally defined as an intentional pattern of repeated...
intrusive and intimidating behaviors toward a specific person that causes the target to feel harassed, threatened, and fearful, or that a reasonable person would regard as being so. What characterizes stalking is the repetitive or systematic nature of the behavior, aimed at a specific person, which is unwanted by the targeted person (Mullen et al. 2001; Van der Aa 2010). The behaviour can be perceived by the victim as annoying, threatening, fear-inducing or disturbing (Van der Aa 2017).

Among researchers there is a broad consensus about the characteristics of traditional stalking: persistent harassment in which one person repeatedly imposes on another unwanted communications and/or contacts (Mullen et al. 2001), stalking is about hunters getting into position to attack and kill their prey (Mathieson 2005). Fortunately, cyberstalking usually has less deadly ends, but there is no doubting the stress and pain victims suffer from such harassment (Mathieson 2005). For cyberstalking, there is no universally accepted definition, but the majority of definitions are based on the assumption that traditional stalking and cyberstalking are essentially the same: cyberstalking is stalking where online technology is used. Cyberstalking, which is the combination of “cyber” + “stalking”, is the prosecution, using various means of communication, the Internet, mobile devices, etc. As part of the definition, the stalking behavior is a form of deviant behavior thus it must be distinguished from offline stalking (out of the Internet).

The terms “cyberstalking” and “intimidation via Internet” must be used interchangeably because all forms of stalking include a threat or an aim to distress victim (victim stress exhaustion). It seems appropriate to link these values to terms such as “stalking” (secret harassment, tracking) and “intimidation” (harassment).

Recently, the crimes of stalking and cyberstalking have received empirical attention; however, few studies have examined the reporting behaviors of victims of these crimes (Reyns/Englebrecht 2010). Researching the issue of cyberstalking the authors define it as anti-social behaviours, potentially with extreme consequences including indirect or direct physical injury, emotional distress and/or financial loss (al-Khateeb/Epiphaniou/Alhaboby et al. 2017). Digital stalking offences frequently termed as acts of cyberstalking (Horsman/Conniss 2015). Such harassments may include the following actions: offensive e-mails sending, personal data theft, equipment or data damage. Cyberstalking means the pursuit of someone by the Internet and other electronic means. Cyberstalking usually involves information collection about a victim by online search service, public attracting and desecrating a person through forums, blogs and social networks.

Cyberstalking may lead to the fact that a cyber-offender – the person who harasses – will pose a real threat to the safety and well-being of victims. In particular, this term can refer to attempts to contact children and teenagers via the Internet for the purpose of personal meeting and further sexual exploitation by adults. This form of cyberbulling is extremely dangerous and can have the most serious
consequences, therefore it is necessary to take all measures to immediately stop it as soon as it was detected. “Cyberbulling” refers to the use of force or influence, directly or indirectly, in oral, written or physical form, or by demonstrating or any other way of images, symbols or anything else usage for intimidation, threats, harassment or embarrassment by the Internet or any other technologies, for example, mobile phones (10 forms of cyberbulling).

Juvenile stalking may signify youth at risk for multiple forms of violence perpetrated against multiple types of victims, not just the object of their infatuation (Smith-Darden/Reidy/Kernsmith 2016). The media has publicized multiple sexting incidents which have resulted in cyberbulling and suicide (Dean 2012). There is also the problem of juvenile suicides committed either directly or indirectly as a result of threats or other forms of incitement to suicide through the Internet. The antisocial activity of organized «groups of death», the participants of which distribute content that contains information about methods of committing suicides and calls for deliberate withdrawal from life, through social networks carries a serious risk of victimization of minors.

In May, 2016 public attention in Russia was riveted on Vkontakte death groups encouraging suicide (reaching the daily audience of 90 mln to exceed the coverage of the First TV channel). A few hundred public pages were constantly renewed (from dozens to millions of subscribers) to spread around the content of largely depressive or aggressive nature, which is close to encouragement of suicide. These activities mostly target young people, especially teenagers. Such situation necessitated the involvement of society and the state in monitoring the behavior of the child in cyberspace (Groups of Death).

Even though cyberbullicide occurs quite rarely in Russia, it still merits proposed and informed prevention and response efforts. According to Federal Service for Supervision of Consumer Rights Protection and Human Welfare (Rospotrebnadzor), during the period from November 1, 2012 to February 1, 2016 its experts have carried out expertizes of 8378 references to websites in the Internet. Experts investigated the maintenance of websites and have found that 8219 links (98,1%) contained prohibited content about ways of committing suicide and (or) appeals to their commission. There was no forbidden content in 159 websites (1,9%) (Official site).

Despite the fact that stalking and cyberstalking outwardly have common features, these terms are not synonymous, so they must be treated properly. Experts earlier noticed that behavioral pathway of stalker referred to the path along which an individual might have progress in moving from communicating with a target to close physical proximity to the target (Meloy 2011). The undertaken study shows that some examples of the main differences between stalking and cyberstalking include the following: the reasons for cyberstalking can be very different unlike offline spanking.
2. Methodology

The methodology of this research consists of general research methods of cognition and special legal methods: formal-legal; analysis; synthesis; logical method; method of legal modelling, and forecasting. The authors rely on general scientific system and axiological approaches to the study of social processes that generate the need to prevent cyberstalking. The methodology of the study includes a review of scientific literature and open information sources, an analytical approach to solving the problem of cybercrime prevention.

3. Reasons of cyberstalking

The corporate stalking assumes that a person, group or organization harasses another person, group or organization. Sometimes reasons for offline stalking can be political or material gain, or competition. For example, disagreements between various competing companies may be associated with the use of illegal methods, hacking computers and providing information to the media.

In general, stalkers always enter into some sort of relationship with their victims. There was not a single case when a stalker has not seen a victim, at least in picture, on TV or in person of the stalking recorded cases.

Cyberstalkers are not limited to small district and can chase victims in other countries with equal ease as if victim lives next door (Bocij 2004). Advanced access and availability of information and communication technology allows the cyberstalker to provoke a third party whom he has never had any relationship, to pursue or threaten another person (Bocij/McFarlane 2004).

It is worth to mention that recently many technologies that are used by cyberstalkers were impossible to employ. For example, the identity theft assumes a simulation of another person for a reason to purchase something fraudulently. However, such actions were impossible in the beginning of new millennium in Russia because only few online shops were using such technology.

The Internet stalking of the eyewitnesses to the crime and their families cause concerns (Krasnova 2015; Losovitskaya/Krasnova/Dyachenko 2010; Kobets/Krasnova 2009). Especially it applies to the witnesses of organizational crimes’ cases on the penal actions (Krasnova/Agapov 2014). According to the best practices the cybersafety of people included in Witness Protection Program becomes the topical issue (Kobets/Krasnova 2009; Ivlieva/Krasnova/Nikolaeva 2015). The secrecy of the witness and his family new names and new place of living, working and studying is one of the main questions that is under concern in Russian and the EU countries (Krasnova 2014a; 2014b; 2015a; 2015b; 2016; Kobets/Krasnova 2015).
The stalking and cyberstalking case study gives the exhaustive idea that stalkers have some psychiatric issues. It is commonsensical, since most of the sources belong to the field of psychology and usually describe only the most unusual cases (Kobets 2005). Nevertheless, it is important to understand that not everyone who is engaged in cyberstalking needs psychiatric help. There is enough evidence supporting the point of view that cyberstalking is only a tool for achieving some goal. Cyberstalking is sometimes used to obtain any financial gain or to overcome competition. Some organized groups attack the opponents using the cyberstalking techniques. The study results allow assuming that the organized hate groups use the Internet to spread disinformation of racial superiority and instigate the violence against people and property.

4. Technological factors of cyberstalking

The next point that we need to review is the technology factors (Kobets 2007b, 18–21). It is assumed that technological factors encourage people to take part in deviant acts, as they allow them to participate there fearless of criminal or administrative sanctions. Technology provides both a tool for a person to act, and the necessary defense from an arrest or another punishment. This discussion starts with the explanation that the technology has become more accessible and easier to use. Moreover, nowadays any ordinary person can hide his identity, actions and destroy any evidence of illegal activity with the help of technical tools.

Although the advanced technologies allow you to extract all the best of technology, nevertheless, the upgrading of software design has the important role in this process. Such upgrade makes the cyberstalkers goal of staying anonymous while committing a crime or deviant acts even easier to achieve. For example, to send an anonymous message by e-mail, he needs some technical knowledge. Users should be able to create relatively complex scripts with instructions that describe how to handle the message. Even if the user can create a script, the whole process of sending messages (especially with attachments) is slow and very unreliable. The incredible Internet expansion caused the appearance of emails re-senders over the Internet. Such possibilities make the sending of anonymous email as easy as filling out a blank on the display. Besides nowadays there are many e-mail pacts that allow to receive the anonymous emails for free (Kobets 2007a, 180–186).

The availability of powerful low-cost software with an encryptor also helps some individuals to remain anonymous and hide their online activities. The same as in the case of anonymous e-mail the software with the encryptor is difficult to use and also it is difficult to get it very often. Implementation of various free encryption packages gives many computer users access to the most powerful of the
available algorithms. There are many investigations of pornography cases where pedophiles used such technologies to hide their activities in many.

Additional protection has appeared for individuals that are involved in deviant acts or criminal offenses as a form of various devices designed to obliterate all traces of their activities on the Internet. For example, there are software packages that erase the details of any website that a user visits, the files that he downloaded, the documents viewed, etc. Files are erased in a way that they cannot be restored by any methods used in judicial practice.

5. Social factors of cyberstalking

Now the social factors are about to be viewed. To consider some social factors that promote motivation for a person and lead him to perform some antisocial or penal online offences (Kobets 2014). Many researchers suggest that Internet anonymity creates a disinhibiting effect that leads to deviant behavior. Face-to-face communication is limited by social norms that control interpersonal interaction, immediate negative reinforcement and the apparent consequences of unacceptable behavior such as public sanctions. On the opposite side, the Internet allows users to communicate in relative autonomy and physical security and keep the distance. Frequently individuals even do not know each other personally and do not realize the negative consequences of such behavior such as risky or potentially damage. It leads to the forms of anger or harassment or to the personal use of socially doubtful material on the Internet, such as pornography (Kobets 2016b, 596–602).

It is logical to assume that the de-individualization process can affect the disinhibiting behavior that is natural to many Internet users. De-individualization is defined as a state when the individual’s self-consciousness is narrowed due to the group affiliation. A person can take part in a criminal act if personal identity is suppressed by the group affiliation. Under such circumstances, a person is sensitive to contextual signals and can participate in behavior that would not take place outside the group. In the utmost conditions the individual’s self-awareness under the influence of de-individualization can lead him to the “herd” behavior (Kobets 2009).

It is reasonable to suggest that various technological features of information and communication technologies encourage psychological and social processes resulting in not exactly normative influence on individuals and groups. In its turn, this leads to more extreme or polarized decisions taken by these individuals. This process includes factors such as the lack of social influence and contextual signals in information and communication technologies, de-individualization, emphasis on the communication context, and not on the social context.
On the other hand it is worth to hear the critics of the statement that many Internet users are de-individualized. It is possible that the alternative explanation of the hostile or aggressive behavior of some Internet users is much more appropriate: the most of the de-individualization effect can be explained without resorting to de-individualization. Anonymity that can appear in the absence of a focus on oneself as a person usually leads to the activation of public identification, rather than personal identification. It may cause the regulation of conduct based on the norms that are connected with a significant social group (Kobets 2015).

There are only few facts known about social and psychological reason for stalking by proxy that is conducted using new technologies. One of the possible explanations is how an individual perceives the power of a group. The group influence and its messages can make him join the group and make him submissive to the proposals and desires of the group. At the same time, the individual clearly expresses the necessity to impose personal responsibility for actions on a third party. At the same time, there is no influence that can incite resistance or outrage (usually by people that are not related to the group).

One can doubt that all these factors can influence on cyberstalking. Firstly speaking about psychological intimacy there are several ways when an individual involved in stalking by proxy in the interests of ultra-right groups can keep the distance with a victim. For example, it has already been said that the emotional connection can be achieved through the protection of anonymity. Secondly, an individual can avoid personal responsibility by pitting it on an extremist group. For example, a person can state that members of the network service forced him to do cyberstalking and it effectively allows him to avoid the guilt of harm caused to others. Finally, a person who often visits extremist network services or chat rooms is practically unable to hear more reasonable and independent points of view than extremist ones. In many cases, such individuals may extensively elude such opportunities, as they lead to cognitive dissonance (Kobets 2016a, 4–9).

6. Understanding cyber-personality

It is considered that the person dismisses thoughts and ideas in artefacts – texts, monuments, work of art (Arkhipov 2011). The media sphere comprises diverse phenomena, such as real and electronic mass media, the Internet, social networking web-sites, forums, etc. that mediate the information transfer between individuals (Baeva 2017). As Fedorova notices,

in mass communication – printed media, television, the Internet – the demand of information shown to the user is provided, and it is guaranteed by the presence of an established contact with the addressee (Fedorova 2016, 108).
Regarding the problem of person’s perception and its cyberspace life, it can be assumed that individuals can create numerous cyber-personalities based on strategic goals. We can assume that the personality is not a static characteristic, but rather it is materialized during the based on the contextual features and roles accepted by the participants who are in this context. With that in mind it is reasonable to assume that Internet user can create several cyber-personalities for different aims. For example, a person working at home can create bottom-line and rational cyber-personality for business conversations and more relaxed and amicable for family and friends’ communications. It is also possible to create the racist cyber-personality for a racist chat room.

This concept seems attractive enough: it can be used to explain the phenomenon of involving a person in on-line deviant behavior and refusing to take part in such acts offline. The creation of the cyber-personality of a cyberstalker allows a person to establish a huge emotional distance between himself and his on-line actions. P. Bocij says that with a little psychological knowledge a con man can start to manipulate us in different ways (Bocij, 2006). Any deviant act committed online can be criminated to a cyber-personality only that releases a person offline from any responsibility for damage or harm caused to others. Let’s note that if some people create an “aggressor” cyber-personality, one can also create a “victim” cyber-personality that becomes more vulnerable or attractive targets.

The difficulties in maintaining the Internet Law enforcement can encourage some individuals for deviant acts or crimes. Without a fear of arrest or prosecution, a person who has never used child pornography offline can download pictures and movies from websites without any hesitation. Similarly, a person who has never been a stalker outside of cyberspace may want to become a cyberstalker. Such acts can take place simply because there is no one who would prevent them (Kobets 2017b, 47–49).

7. Conclusion

It is well known to criminologists that all actions usually have three present elements such as a possible criminal, a suitable target (goal) and the absence of someone who is able to deter from committing a crime (Kobets 2005b, 61–67). There are also three important elements such as characteristics of a crime: requisites (for example, tools), camouflage (to help the offender to go unnoticed) and the audience that the offender wants to affect or frighten. Not much effort should be taken to discover all these elements as for the wrongful acts committed by cyberstalkers. In fact, many of them were above-mentioned but in other terms. For example, requisites (in the form of computer equipment, software and services) and camouflage (in the form of anonymous e-mail, encryption and other methods) were discussed.
The notion of one who is able to deter from crime is of great importance in this context. It is not necessary a policeman who keeps from committing a crime or prevents a crime, but it can be any person. Moreover, its absence makes possible to commit a crime. To show how the issue can be applied to areas such as cyberstalking, you can use an example of chat rooms where the active communication of Internet users takes place. The majority of parents prefer their children to use moderated chatrooms. Due to the fact that the moderator presence helps to protect children from negative effects in various ways. For example, moderator can frighten pedophiles or counter the bullying (psychological terror).

In the conclusion we would like to note that there are much more factors that can explain why some individuals are involved in the Internet illegal actions. The authors acknowledge the public danger of cybercrime and the necessity to find the best ways to prevent it.

Future studies should exchange expertise, such as, but not limited to, best practice, statistical data, technical information or cybercrime trends between Central and Eastern Europe and Russia. Experts can continue explore the social conditioning of criminal law prohibitions in cyberspace and observe the necessary conditions for criminalizing dangerous behavior in cyberspace.

References


KOBETS, P. N. (2005a), Consideration of relevant legal aspects of the use of methods of applied psychology in the investigative practices of law enforcement bodies of the Russian Federation in the classroom with law students. In: Volkov, E. V. (Ed.), Psychological and pedagogical support of the educational process in higher education and ways to improve it, 103–108. Moscow. (In Russ.).


KOBETS, P. N. (2007b), The main factors which contribute committing crimes of an extremist nature on the part of religious totalitarian sects operating in Russia. In: The Russian investigator. 22, 18–21. (In Russ.).

KOBETS, P. N. (2009), The use of psychological methods of arrangement of memory of victims, witnesses and suspects in investigative practices of law enforcement bodies of the Russian Federation and foreign countries. In: Legal psychology. 6, 10–14. (In Russ.).


KOBETS, P. N. (2015), About the concept the identity of the offender, as one of the important problems of criminological science. In: Ashmarina, S. I. (Ed.), Fundamental and applied studies in the modern world. 4, 90–92. Sankt-Petersburg: Information and publishing educational and scientific center “Strategy for the future”. (In Russ.).

KOBETS, P. N. (2016a), About modern information technologies used by extremist groups, and the need to counter cybercrime. In: Bulletin of development of science and education. 6, 4–9. (In Russ.).


KOBETS, P. N. (2017a), The threats of cyberstalking – the most important problem studied in the framework of improving aspects of information security of regions in the conditions of globalization of information space. In: Bulletin of Prikamsky Social Institute. 1 (76), 27–35. (In Russ.).

KOBETS, P. N. (2017b), The use information resources by law enforcement authorities for counteraction to human trafficking. In: Matrix of scientific knowledge. 2, 47–49. (In Russ.).

KOBETS, P. N./KRASNHOVA, K. A. (2009a), About an indemnification problem to the victim at a stage of preliminary investigation. In: Criminal procedure. 4, 30–33. (In Russ.).

KOBETS, P. N./KRASNHOVA, K. A. (2009b), Problems of compensation of harm to the victim at the preliminary investigation stage. In: Lawyer’s practice. 6, 76–94. (In Russ.).


KRASNHOVA, K. A. (2015b), Witness protection in the member states of the EU. In: International law. 4, 66–86. (In Russ.).


