

BRUNON HOŁYST



CYBERSTALKING AS A FORM OF CYBERHARASSMENT

1. Legal essence of cyberstalking

The phenomenon of cyberstalking is defined as the use of the Internet or other means of communication in order to harass an individual, a group or an organisation¹. It may include a wide range of activities having adverse effects on and detrimental to a victim². Although cyberstalking differs from classic stalking as it uses electronic media, both forms of harassment often occur together and perpetrators are motivated by the need to control their victims³. Cyberstalking is treated as a form of cyberharassment and both forms are nowadays treated as crimes.

Cyberstalking is one of the forms of stalking. The dangers that this form of harassment carries were noticed for the first time in the USA at the early 1990s, which resulted in the regulation of a perpetrator's behaviour in both state and federal law. In 1999, Attorney General sent a special report to Vice-President A. Gore, in which he highlighted threats connected with Internet communication. The crime carries a penalty of five-year imprisonment and a fine of \$250,000. Moreover, in 1998, President B. Clinton signed anti-stalking law. In addition, many governmental and non-governmental organisations were founded to provide support for victims⁴. It is essential because stalkers act more and more frequently. For example, a 50-year old security guard in California was convicted on a charge of using the Internet to rape a woman who rejected his romantic advances. The accused terrorised an almost 30-year old woman by acting on her behalf in chat-rooms, on the Internet and advert boards where he published her telephone number and address. He also sent messages on her supposed desire to be raped and signed them on her behalf, which resulted in numerous intruders' visits to

¹ P. Bocij, *Cyberstalking: Harassment in the Internet age and how to protect your family*, Praeger Press, Westport C.T., 2004.

² B. Loader, *Cybercrime: Law enforcement, security and surveillance in the information age*, Routledge, London 2000.

³ S. Furnell, *Cybercrime: vandalizing the information society*, Addison Wesley, London 2002.

⁴ *Working to Halt Online Abuse* (www.haltabuse.org).

the woman's house. The accused pled guilty and was sentenced to six years' imprisonment. In San Diego, a stalker terrorised students via the Internet and his victims received hundreds of threatening emails, sometimes tens of them per day. The perpetrator wanted to take revenge for being laughed at, as he thought, but in fact, the victims had never even spoken to him.

Canadian anti-stalking legislation entered into force in 1993 and it envisages that "Nobody can be constantly afflicted by letters, surveillance of the dwelling or workplace, or threats against oneself or one's family that endanger their physical or psychological security". However, for the first time in history, stalking was recognised as criminal activity in California, in the US, in 1998⁵. It was decided that the law of that state should ban stalking and expressing threats against other persons if these make them feel that there is safety hazard to them and their families. In case of cyberstalking, the threats are transmitted via the Internet, email, telephone (also a cellular one), facsimile, video or any other electronic means of communication. The definition of the concept of "threat" was amended in California and now it covers a "threat transmitted in the form of an electronic transmission"⁶.

The term stalking covers a series of specific behavioural activities. They include, inter alia, false accusation that aims to ruin a victim's reputation. The accusations are published in various places on the web, such as blogs, social networking sites etc. Cyberstalkers collect information on their victims, their family, friend, the surrounding etc. They look for that information online and sometimes hire specialists, e.g. private detectives. The perpetrators monitor their victims' online behaviour in real time (on line) and try to steal their personal passwords, and this way gain access to private information⁷. One of the signs of cyberstalking is encouraging other people to harm a victim; to this end, they present their victim as a person guilty of many evil deeds, provide the victim's personal data, photographs, address, telephone number, etc. They often present the victim as their stalker. Cyberstalking sometimes takes the form of infecting the victim's computer with viruses and sometimes in ordering – on a victim's behalf – various goods such as erotic gadgets or pornographic magazines subscriptions, which are then delivered to a victim's house. In case of young people, cyberstalkers often strive to arrange real-life meetings⁸.

⁵ California Cyberstalking Laws (<http://www.shouselaw.com/cyberstalking.html>) (29.11.2013).

⁶ *Cyberstalking crime research* (<http://www.crime-research.org/library/Cyberstalking.htm>).

⁷ P. Bocij, *Cyberstalking: harassment in the Internet age and how to protect your family*, Praeger Press, Westport C.T., 2004, pp. 9–10.

⁸ D. Sarzała, *Problem agresji i przemocy w mediach elektronicznych – aspekty psychologiczne i etyczne* [Problem of aggression and violence in electronic multimedia – psychological and ethical aspects], [in:] J. Bednarek, A. Andrzejewska (ed.), *Cyberświat – możliwości i zagrożenia* [Cyberworld – possibilities and threats], Wyd. Akademickie "Żak", Warszawa, pp. 243–273; also compare B. Hołyst, *Bezpieczeństwo społeczeństwa* [Community security], vol. III, PWN, Warszawa 2015, p. 586 and the following.

According to an American website involved in the research into stalking phenomena (www.stalkingvictims.com), almost 1.5 million Americans have been affected by this problem. The perpetrators of stalking are usually men (66–90%). But both men and women look for a victim among persons representing the opposite sex, thus the background is erotic. Stalking is committed against representatives of the same sex less frequently. Perpetrators are usually middle-aged (30–50 years old), but there can also be younger persons, e.g. 15-year-olds, and in extreme situations even 9–11-year-olds⁹. Contrary to a common belief, it does not concern only stars or celebrities. The victims are also ordinary people, however, their cases are not well-known ones because the media are not interested in publicising them. In one case a stalker harassed a female colleague for four years. He was dismissed from work and ordered to refrain from intimidating her. The perpetrator ran amok, entered the workplace, shot seven persons and injured four (including the woman he used to harass). In another similar case, an emotionally disturbed woman attacked a well-known American TV showman, David Letterman of the CBS. The woman believed that the famous comedian was her husband and harassed him for a few years. In 1998, G. Dellapenta from Los Angeles published the genuine personal data on the web, including the address and telephone number of his former partner who left him. Then, pretending to be her, he announced that she was in favour of very shocking forms of sexual intercourse and started to demand them from her. Six other men responded to the encouragement. The man was brought before court and sentenced to six years' imprisonment¹⁰.

As it was mentioned, the first American state to pass anti-stalking law was California and the reason behind that decision was a series of stalking-related murders, e.g. in 1982 attempted murder of actress Theresa Saldana, and a massacre by Richard Farley in 1988. The first regulations were laid down in the criminal law of California on the initiative of Judge John Watson of Orange County, who together with senator Ed Royce led to passing the anti-stalking bill¹¹. The states of Alabama, Arizona, Connecticut, Hawaii, Illinois, New Hampshire and New York developed and implemented anti-stalking programmes. The states of Alaska, Florida, Oklahoma, Wyoming and California revised their legal regulations and introduced formal bans on stalking (especially cyberstalking) and started treating it as a crime. Texas started developing a protective system and legal regulations against cyberstalking and as a result, Electronic Communication Act was passed in 2001.

⁹ www.stalkingvictims.com

¹⁰ J. Kosińska, *Prawnokarna problematyka stalkingu* [Legal-penal issue of stalking], *Prokuratura i Prawo* 2008, no. 10, pp. 33–47.

¹¹ *Cyberstalking: A new challenge for law enforcement and industry: A report from the Attorney General to the Vice President*, Washington DC: US Department of Justice, 1999.

In-depth research into the phenomenon was carried out in Canada¹². The first stalking case was reported there in 1993 and it was an impulse to regulate the issue in the Criminal Code of Canada. The research conducted by the police and psychologists resulted in the development of psychological profiles of perpetrators. In Ontario, there are many organisations combating stalking and promoting the idea of anti-stalking regulations and measures to fight against the phenomenon. The organisations provide legal information with the use of a website called Ontario Women's Justice Network, which records a few hundred hits daily. New regulations on stalking were also passed in Australia in 2008. Personal & Domestic Violence Act was developed to regulate the issue of stalking as a crime. In addition, people are encouraged to have the so-called Apprehended Violence Order, which contains standards concerning the assistance to victims, necessary addresses and telephone numbers of dedicated police helplines dealing with stalking. The US Department of Justice webpage also provides a lot of information on stalking, in particular its definition and tips on how to combat cyberstalking with special attention paid to the specificity of electronic communication means such as a telephone, a facsimile, GPS, cameras, computers and Internet links¹³. The Stalking Resource Center of the National Center for Victims of Crime plays an important role in the field¹⁴.

The crime of stalking, including cyberstalking was regulated in the Polish Criminal Code in Article 190a:

- § 1. Whoever persistently harasses another person or his next of kin, and causes in the harassed person a justified fear of danger or substantially infringes his privacy shall be subject to the penalty of up to three years' imprisonment.
- § 2. Whoever pretends to be another person, uses his image or other personal data in order to cause financial or personal damage shall be subject to the same penalty.
- § 3. If the act referred to in § 1 or 2 results in a victim's attempt to commit a suicide, the perpetrator shall be subject to the penalty of one to ten years' imprisonment.
- § 4. The prosecution shall occur on a motion of the injured person.

It is worth reminding that earlier, i.e. before the amendment to the Criminal Code was passed, Article 31 of the Constitution of the Republic of Poland constituted grounds for whatever liability of a perpetrator of stalking. There is no doubt that stalkers' activities are aimed at the legal good that is a person's freedom. With regard to the provisions of the Criminal Code that might have

¹² J. Kosińska, *Prawnokarna problematyka stalking* [Legal-penal issue of stalking], *Prokuratura i Prawo* 2008, no. 10, p. 43.

¹³ *Cyberstalking: A new challenge...*, *op. cit.*

¹⁴ J. Woźniak, *Stalking jako rodzaj uzależnienia emocjonalnego i uczuciowego od osoby* [Stalking as a type of emotional and sentimental dependence on a person], www.psychologia.net.pl.

been referred to in case of such conduct was Article 207 of the CC referring to harassment meant as activities consisting in inflicting physical or psychological suffering, using violence, threatening and insulting a victim. Harassment has the form of single- or multiple-type activities that infringe the freedom or dignity of the harassed person. Exceptionally, harassment can also be an activity that, although it is limited to a single event in terms of time or place, is very intensive in terms of physical and psychological suffering, especially one composed of many acts performed in an extended period of time. According to the Supreme Court, the verb feature “harasses” means that the misdemeanour is performed repeatedly, although in an extraordinary situation, one occurrence of this type of conduct is sufficient. The provision lays down who is subject to protection: the next of kin or other persons who are in permanent or temporary dependence relationship with the perpetrator or minors, or incapable persons because of their physical or psychic condition. Such persons are most often a stalker’s victims. However, the range of people who may be victims of this crime was limited in comparison to the situations in which persistent harassment occurs, because a stalker acts against any person he knows as well as an accidental victim. Thus, protection provided by the same provision did not cover all the situations in which the earlier relationship between a stalker and a victim can be classified as being just acquaintances or when a perpetrator is a stranger.

According to J. Kosińska, the Supreme Court rightly defined the dependence relationship as a situation in which a victim is a perpetrator’s dependant because he is not capable of resisting harassment on one’s own and suffers it because of a fear that his present living conditions might deteriorate into, e.g. a loss of the job, income or dwelling, the separation or the severance of sex life with the perpetrator¹⁵. It can also result from the real-life situation creating circumstances in which a perpetrator harasses a victim using the advantage over a victim, which he gains thanks to material, personal or emotional relationship between them. A perpetrator most often refers to this relationship. Article 207 of the CC covered a too small range because it did not refer to situations when a perpetrator and a victim are just acquaintances or have no relations at all. According to the research findings, persistent harassment takes place in situations in which there was a close relationship between a perpetrator and a victim, but there is also a big percentage of cases in which, e.g. because of psychic disorder, a stalker is a complete stranger. The essence of the crime of harassment consists in a stalker’s qualitatively different conduct than only insulting or physical abuse of a victim. A perpetrator’s behaviour is not limited to an event that is systematic or occurs in a certain limited place or time. Most often, it is connected with the intensity, severity and excessive insult as well as the aim of single acts infringing particular goods, e.g. dignity or bodily inviolability.

¹⁵ Resolution of the Supreme Court of 9 June 1976, VI KZP 13/75, OSNKW 1976, no. 7–8, item 86.

In every specific case, it is necessary to assess the situation from an objective point of view, using a model citizen (or an average ordinary man), i.e. a man with an appropriate level of socialisation and sensitivity to another person's harm¹⁶. This model citizen is necessary to interpret a perpetrator's intention. A stalker's behaviour may demonstrate the features of a crime of a punishable threat, especially in case of stalking or forcing to act in a particular way. Article 190 of the CC defines a punishable threat, which infringes a man's freedom in the psychic sphere (freedom from fear); it deals with threatening another person with a crime (a felony or a misdemeanour) harming him or his next of kin. The Supreme Court decided that a punishable threat might be expressed through any type of a perpetrator's behaviour (a verbal or written announcement or expressed in a gesture, e.g. aiming a gun at a person etc.) if it undoubtedly demonstrates a threat of a crime commission. The condition for classifying an act as a criminal one is that a threat causes justified fear that it will be fulfilled. It should be interpreted as a situation in which a victim treats a threat seriously and believes it can be really fulfilled.

A perpetrator influences the psyche of another person by presenting a threatened person the wrong that is going to happen to him/her unless he/she does what the perpetrator wants. A perpetrator does not have to really intend to fulfil his threat; it is enough that the content of his threat is passed to a threatened person. A victim's subjective conviction that there is a possibility that a threat will be fulfilled must be justified, i.e. the circumstances in which a threat was expressed as well as a perpetrator's activeness make a victim believe that a threat is serious and gives grounds to fear. The issue was discussed in court decisions that state that a crime under Article 190 takes place if it can be proved that a threat induced a subjective (perceived by a threatened person) fear that it will be fulfilled and then verified (by court) whether a threatened person could really have perceived that threat in this way in the given circumstances¹⁷.

Article 190 of the CC lays down the means of threat that are violence towards a person or a criminal threat. Violence is such influence with the use of physical force that precludes a threatened person from taking or implementing their free will decisions, or affecting a person's motivational processes by affliction to induce a victim to take a decision desired by a perpetrator. The use of violence consists in a broadly understood physical action performed directly against the injured party, which is aimed at enslaving them and make them submit to a perpetrator's will or behave in a given way, or against another person. Violence used then, most often through a victim's emotional relationship with a perpetrator, may

¹⁶ J. Kosińska, *Prawnokarna problematyka stalkingu* [Legal-penal issue of stalking], Prokuratura i Prawo 2008, no. 10, p. 38.

¹⁷ Sentence of the Court of Appeal of 4 July 2002, II AKa 163/2002, KZS 2002, no. 7-8, item 44.

lead to enslavement and submission to a person using violence¹⁸. The Article is a useful solution in combating the discussed crime because it does not contain a requirement for a victim to be the next of kin and other conditions for the type of relationship with a perpetrator as referred to in Article 207 of the CC¹⁹. On the other hand, it includes only the use of violence or a criminal threat in the features determining the causative act. They are means to achieve a perpetrator's planned objective, thus a crime can be committed only in case of a direct intention. Taking into account the features of forcing a victim to act in a given way, it seems that a perpetrator corresponds to one defined in Article 191 § 1 of the CC. A stalker, intentionally, with the use of different methods, forces a given person to behave in a given way, to submit to a perpetrator's will or to give up some activities, e.g. keeping in touch with persons other than a perpetrator, and also forces a victim to accept the relationship between them by using violence or a criminal threat.

Act of 29 July 2005 on combating domestic violence²⁰ is an important regulation with respect to combating stalking. The statutory protection covers family members, i.e. the next of kin as well as other persons who reside together with or are members of a the same household as a person using violence. The legislator understands domestic violence as occasional or repetitive intentional activities or omissions infringing the legal and natural rights of persons specified in the statute, especially endangering these persons' life, health, dignity, bodily inviolability, freedom, especially sexual one, causing harm to their physical and psychological health as well as inflicting the feeling of suffering and moral wrong upon victims of violence. Persons whose behaviour is classified as domestic violence are subject to the use of measures aimed at preventing them from having contact with their victims and influencing them with correctional and educational methods. The statute also envisages a range of assistance measures that may be addressed to victims, including, inter alia, psychological and legal counselling, crisis intervention and a safe shelter in a specialist centre. Apart from the above-mentioned measures, the statute introduces a certain innovation in the procedure of conditional discontinuation of the criminal proceeding and in the suspension of the execution of a punishment towards a perpetrator of a crime committed with the use of violence or a criminal threat against a member of his family.

The above-mentioned statute amends the Criminal Code and envisages that a court imposing an obligation to refrain from contacting victims or other persons in a particular way and to leave the dwelling used together with a victim,

¹⁸ A. Barczak-Oplustil et al., *Kodeks karny. Część szczególna, t. II: Komentarz do art. 117–277* [Civil Code – Specific issues, vol. II: Commentary on Articles 117–277], Zakamycze, Kraków 2006.

¹⁹ J. Kosińska, *Prawnokarna problematyka stalkingu* [Legal-penal issue of stalking], *Prokuratura i Prawo* 2008, no. 10, p. 38.

²⁰ *Journal of Laws* No. 180, item 1493.

obligatorily determines the way in which a perpetrator may contact a victim and optionally imposes a ban on approaching a victim in given circumstances. In case there are grounds for the application of temporary arrest towards the accused of a crime committed with the use of violence or a criminal threat, a court may rule intensive probation by the police provided that the accused leaves the dwelling used together with the victim until the deadline determined in the court decision and provides information about his new place of residence. The provisions of the discussed statute let a court impose an additional punishment on the accused in case he leaves the place of residence. It is worth remembering that the harassed victims suffer from the consequences of stalking for a very long time. The time when a perpetrator is in prison may be the time of peace and quiet for his victims. But there are cases when a perpetrator attempts to continue harassing his victim from prison, e.g. sending letters.

In a similar way as in American regulations, Polish Penalties Execution Code envisages a possibility of informing victims about the fact that a perpetrator has left prison. Under Article 168a of the PEC, on a motion filed by a victim, a penitentiary judge or the head of prison without delay notifies a victim, his legal representative or his legal guardian about the release of the convict after having served the punishment, about the escape of the convict from prison and also about granting the convict a pass, temporary release from prison without intensive probation or without escorting by a prison officer or another trustworthy person, a break in the execution of a punishment and conditional release. The provision plays a very important role, especially in cases of persistent harassment because a victim can get psychically prepared for the possible meeting with the former stalker. Such a notification can occur only on a victim's motion and refers also to a convict's release from prison after having served the whole punishment and a convict's escape from prison²¹. The organs obliged to notify a victim should know that a victim has been informed and has filed an adequate motion in the court that has informed him about the right. J. Kosińska emphasises that the introduction of a monitoring programme would contribute to the improvement of a victim's state of mind and the increase in the supervision of a perpetrator's conduct in the period of probation²².

According to the cited author, it would be a good idea to introduce the so-called register of stalking cases into the daily work of law enforcement agencies. It would be used to collect information about a victim and a perpetrator's data; it would include information about witnesses, circumstances and a perpetrator's modus operandi. An introductory section would concern a victim, who would provide his/her first name, surname, sex, date of birth, address, telephone number

²¹ Z. Hołda, K. Postulski, *Kodeks karny wykonawczy. Komentarz* [Penalties Execution Code – Commentary], Zakamycze, Kraków 2008.

²² J. Kosińska, *Prawnokarna problematyka...* [Legal-penal issue...], *op. cit.*, p. 40.

and profession. Information about a perpetrator (with a photograph) would include his/her false name, sex, date of birth, address, frequently visited places, telephone numbers used in contact with a victim, email address, profession, workplace and his/her employer's data. Moreover, it would be necessary to collect information about a perpetrator's car (registration plate number, colour, model, make) and check if he/she carries a gun or has been granted a firearms license. Important information concerns a perpetrator's past, earlier criminal record and classification of committed crimes. A description of an event may include the date, the part of the day (time), the venue, the potential witnesses and the possibility of contacting them, and the course of the event (information or evidence a perpetrator has left). Successive events can be recorded in the same way and thus evidence can be collected. The collection of all the information may be easy if a victim knows a perpetrator from workplace or private circles and it is possible they will know his/her co-workers, acquaintances etc.

2. Role of the Internet in stalking

It is highlighted that proceeding against stalkers may encounter specific problems²³. The Internet is a means of mass communications when it is used to transfer information to strictly specified or non-specified, but numerous entities that can be attributed a name: "multiplicity of recipients". The Internet adopts this character when, e.g. the content has been entered into a forum of a given Internet service or on a website (World Wide Web). A given website is available to an unlimited number of entities that may visit that Internet site²⁴. The analysis of a given actual state leading to a conclusion that in order to commit the crime of stalking consisting in defamation or insult, the Internet has been used as a means of facilitating the distribution of the content banned by the provisions to an indefinite number or a definite but substantial number of recipients results in the necessity to treat the medium in this situation as "a means of mass communication" as referred to in Article 212 § 2 of the CC and Article 216 § 2 of the CC. As a result, in such a situation, a perpetrator commits an act that has the features of an unlawful act in its aggravated form.

In the field of communication and transfer of information between people, the Internet nowadays offers possibilities of sending information by electronic mail to a single person or a limited number of people (so that it does not have the feature of being "public" as referred to in the provisions of the CC cited above), the so-called email and instant messaging systems. Electronic mail is

²³ T. Fołta, A. Mucha, *Zniesławienie i znieważenie w Internecie* [Defamation and insult on the Internet], *Prokuratura i Prawo* 2006, no. 11, pp. 49–63.

²⁴ M. Sowa, *Ogólna charakterystyka przestępczości internetowej* [General characteristic of Internet crimes], *Palestra* 2001, no. 5–6, p. 31.

a system of message and data transmission between computers via the Internet links. The system can be used to send text messages as well as all types of computer files. On the other hand, instant messaging is a program that offers real-time direct online chat with another person (inter alia, GaduGadu, Tlen, AOL Instant Messenger, Hello). The conversation takes the form of short texts transmission. The transmission of the content that is defaming or insulting in character is not different from a traditional letter written on a sheet of paper and sent to a particular person or an oral transmission of that content during a face-to-face or telephone conversation²⁵. One can compare the crime of defamation committed with the use of a letter sent by post and sent as an email. A keyboard substitutes for a pen, a monitor substitutes for a sheet of paper, an email address substitutes for a home address, and cables and optical fibres substitute for postmen.

Computers creating the Internet network serve as transmitters of information included in an email in the same way as the post office, which acts as a middleman in the delivery of a physical letter. Thus, the use of the above-mentioned Internet tools cannot constitute “public” transfer of information that would be an aggravated form of unlawful acts subject to the provisions of the CC cited earlier. In case this condition is fulfilled, the use of the Internet to transfer defaming or insulting information in the above-mentioned way does not make the medium “a means of mass communication” because the content transmitted is not addressed to such a group of people that would cause “public” defamation or insult. Such content, in such a situation, is addressed to a strictly defined person or a limited group of people (e.g. an email to the company board). The use of the Internet by a perpetrator as “a means of tightly closed interpersonal communication” during the commission of a crime of defamation or insult causes that this conduct has the features referred to in the above-mentioned Articles of the Criminal Code.

Thus, the Internet used for such communication does not become a tool aggravating the type of an unlawful act and its use is not a feature of the basic type of crimes discussed here. It is of great practical importance for the use of the legal classification of a given act. It directly influences the proceeding-related situation of a perpetrator because the aggravated type of crime, both defamation and insult, carries a more severe punishment. The classification of the Internet – in one of its forms – as “a means of mass communication” making it a feature of the aggravated type of an unlawful act has been dictated by the fact that it has, like such media as radio, the press, television and even posters with unlawful content displayed in commonly accessible public places, extraordinarily wide opportunities to reach practically unlimited number of

²⁵ T. Foltá, A. Mucha, *Zniesławienie i znieważenie...* [Defamation and insult...], *op. cit.*, p. 52.

people with the transfer of information²⁶. On the other hand, the Internet provides opportunities to communicate individually without the mass character of the recipients of the transferred content. In such a situation, the medium goes beyond the term “a means of mass communication” and becomes a different type of means of communication, namely “a means of tightly closed interpersonal communication”²⁷.

As it was mentioned before, in case of stalking, we very often deal with defamation and insult. Both defamation and insult belong to crimes that are subject to private lawsuit and, taking into account their character, the legislator envisaged a special mode of proceeding in such cases. Its characteristic feature is that, inter alia, a victim or persons that can act on his behalf have the entitlements of a prosecutor. A victim may file and support an indictment until the time limit for a given crime limitation. There are numerous Internet services like forums, discussion groups, chat-rooms, guest books, blogs etc. where the content entered by a user (opinions, beliefs, information) become publicly accessible for an unlimited number of people²⁸. Users can publish their own content in fact freely deciding on how it should be signed. Usually, they sign it with a pseudonym. It ensures being anonymous and provides the Internet users with the conviction of impunity²⁹. Resulting from the general rules of the Internet connections, information included in the logfiles that can be helpful in identifying a perpetrator are retained and used by server administrators mainly for technical and administrative purposes. Data necessary to open an email account – an email address – or instant messaging are not verified whether they are genuine and they are not revealed to third parties.

All computers directly linked to the Internet have their unique IP address (Internet Protocol address) individually assigned to each device. The address consists of four 8-bit numbers, each with values ranging from 0 to 255. It is a “registration number” of a given computer and every part of the address means something different and makes it possible to establish a smaller and smaller area where a computer can be found. Thus, by using one part, a given network can be established, with the use of another one a subnet can be specified within the network, and next a computer can be located in the network. Such a structure results from the specificity of the IP. The scopes of addresses constituting the so-called classes are assigned to companies providing Internet access services.

²⁶ A. Zoll, *Kodeks karny. Komentarz. Część szczegółowa* [Criminal Code – Commentary – Detailed issues], Zakamycze, Kraków 1999, p. 647.

²⁷ T. Fołta, A. Mucha, *Zniesławienie i znieważenie...* [Defamation and insult...], *op. cit.*, p. 54.

²⁸ J. Bednarek, *Teoretyczne i metodologiczne podstawy badań nad człowiekiem w cyberprzestrzeni* [Theoretical and methodological bases of research into man in cyberspace], [in:] J. Bednarek, A. Andrzejewska (ed.), *Cyberświat – możliwości...* [Cyberworld: opportunities...], *op. cit.*, pp. 23–55.

²⁹ J. Szwarz, *Prawne aspekty przestępczości teleinformatycznej* [Legal aspects of telecommunications crime], [in:] J. Bednarek, A. Andrzejewska (ed.), *Cyberświat – możliwości...* [Cyberworld: opportunities...], *op. cit.*, pp. 355–374.

Thanks to its uniqueness, the IP address – together with the exact time of a connection – unambiguously identifies the device on the web and the company it comes from. In order to read a particular IP address, it is necessary to have the logfiles (digital ones) of the Internet servers. A logfile is the information that a computer transfers to the server at each instance of a connection to the Internet³⁰. Logfiles register data on the activeness of their clients on the web and make it possible to determine which sites on the web they linked to, where they sent messages, where from and when they received them and what kind of transactions they made. This is such information as e.g. a transfer of files (sending and downloading), participation in a discussion group or a visit to a www site. The register files are generated by the providers of access services and include data that can be an “electronic trail” of perpetrators of various crimes committed with the use of a computer, including stalking.

The discussed procedures are especially important in case of the Internet users who are not connected to the web permanently but use the so-called communication protocols enabling them a temporary connection to the Internet with the use of a modem or a telephone. Once a modem connection to the access provider starts, its server automatically assigns a subscriber an IP address from the so-called address pool available to the Internet providers for allocation to users³¹. The signal with information is sent with the use of, more or less, the same elements as a telephone conversation. Each time an owner of a modem wants to connect to the Internet, the telephone network operator assigns him an IP number. It is a number that is not assigned to a particular user forever. It is assigned to a user for the time of his activeness on the web. In order to match a computer with the IP address, it is necessary to match the date and the time with the user of the given address. Thus, any activeness of a given computer in the web is related just to its address³².

3. Identification of stalkers

The so-called telephone billings, which contain information about the subscriber's station number, the subscriber's address, the number of telephone units used by the subscriber in a billing cycle, telephone numbers the subscriber was connected to, dates of connections, the length of the connections and their type (international, national, local ones or to the Internet). The provider is obliged to register the data concerning communications services provided in the scope

³⁰ M. Kliś, A. Stella-Sawicki, *Identyfikacja użytkownika komputera na podstawie logów cyfrowych* [Identification of a computer user based on digital logfiles], *Prokuratura i Prawo* 2001, no. 7–8, p. 52.

³¹ A. Adamski, *Prawo karne komputerowe* [Criminal computer law], Wyd. C.H. Beck, Warszawa 2000.

³² M. Kliś, A. Stella-Sawicki, *Identyfikacja użytkownika...* [Identification of a computerer...], *op. cit.*, p. 53.

that is necessary to calculate the charge for the services³³. It must be emphasised that some local computer networks use the mechanisms of dynamic allocation of the IP address, i.e. assigned for each connection to the Internet individually. This may complicate matching the given IP address with a particular computer that used it on the web. Billing data, as information about communication connections between subscribers' stations, are shrouded in communication secrecy under Act – Telecommunications Law of 16 July 2004³⁴. Revealing this secret information may take place only based on a court or a prosecutor's decision, or based on other regulations.

Every web user may also create one's own website and enter it onto the web, and present whatever content he wants, including one defaming or insulting another person. The sites constitute a wide range of linked documents and other files located in other computers that are connected via the Internet and make it possible to access, use and copy the information, data and programs. In order to be used by other web users, they must be saved in a form of a computer file on a server's hard disc, i.e. a computer that, in most cases, is not owned by the owner of the site. A space on a server is offered by many firms for a fee but also free of charge. A victim may on one's own try to detect a perpetrator of a crime of defamation of insult. However, choosing this way, from the very start, he is doomed to failure because a victim harassed by another web user may only know his Internet pseudonym, email address or the number of instant messaging system. In order to obtain an IP address or personal data of a given IP address user who with the use of the Internet committed a crime referred to in Article 212 of the CC or Article 216 of the CC, a victim must apply to the administrator of the server on which there is a forum where an insulting message was entered and demand the release of the IP address matching the given content. Due to the fact that in most cases a server administrator does not have other personal data (a first name, a surname, an address) of the user, it is necessary to apply to the Internet services provider of the established IP address to provide the information. However this information is protected by Act on the protection of personal data of 29 August 1997³⁵.

According to law, personal data may be provided to third parties only if they justify the need to have these data in a trustworthy way and their provision does not violate the rights and freedom of a person they concern. The data are provided based on a written, substantiated motion that should contain information that make it possible to find the data as well as indicate their scope and purpose they are to serve. However, one of the articles of the discussed statute entitles the administrator of personal data to refuse to provide them.

³³ A. Lach, *Dowody elektroniczne. Pojęcia i klasyfikacja* [Electronic evidence: Concepts and classification], *Security Magazine* 2001, no. 4, p. 24.

³⁴ *Journal of Laws* of 2004, No. 171, item 1800.

³⁵ *Journal of Laws* of 1997, No. 133, item 883.

It must be added that the refusal does not have the form of an administrative decision or a ruling³⁶. It is a written reply that is not an act or action within public administration procedures that concern granting, determining or recognizing an entitlement or an obligation resulting from legal regulations. In case of such a refusal, a victim may initiate a proceeding before the Inspector General for Personal Data Protection, which is a special and the only mode of adjudicating in the field of personal data. In case of a negative decision of the IGPD, a victim may file a complaint to the Voivodeship Administrative Court. A much more serious problem arises when a cyberstalker slandering a victim's good name connects to the web with the use of a modem or a telephone and is assigned a temporary IP address. In such a case, it is necessary to apply to the telecommunications operator in order to obtain billing data, however, these are protected by communication secrecy. In such a case, a victim may only have an IP address, which is not sufficient to file a simplified indictment. In accordance with the provisions, such an indictment must contain at least the determination of the accused, a description of an act he is charged with, and the indication of evidence supporting the indictment. The determination of the accused should provide an opportunity to individualise him to deliver him a summons, thus it should contain the accused's given name, surname and address³⁷. Both an IP address and email address are not such an individualisation of the accused, which results in ineffectiveness of such an indictment.

In case a victim chooses a different way of vindicating his rights and files a complaint to the police, unlike in case of a simplified indictment, this complaint does not have to contain the data of the perpetrator of an unlawful act as establishing them is the role of the police. To this end, the police do not initiate a formal preparatory proceeding, an investigation or an inquiry, they do not conduct a proceeding in the indispensable scope or an explanatory proceeding, but start procedures, complying with all envisaged rigours, aimed at protecting evidence. Protecting evidence may be connected with looking for evidence and activities aimed at detecting a perpetrator of a crime. It is emphasised that the Criminal Procedure Code does not directly determine what activities the police should undertake within their entitlements. Taking into account the system interpretation, it seems that the legislator introduced some kind of agencies' authority gradation depending on the type of the proceeding before a trial starts.

The broadest proceeding entitlements are connected with an investigation, a little smaller in case of an inquiry, and there are numerous objective restrictions in case of an explanatory proceeding. The objective scope of the police activities is narrower and includes checking the identity documents of a person indicated by

³⁶ T. Folta, A. Mucha, *Zniesławienie i znieważenie...* [Defamation and insult...], *op. cit.*, p. 57.

³⁷ T. Grzegorzczak, *Kodeks postępowania karnego. Komentarz* [Criminal Procedure Code – Commentary], Zakamycze, Kraków, 2004, p. 1245.

a victim, establishing his name and address, scene of crime or body examination, establishing names and addresses of witnesses, interviewing witnesses, especially those who will not be able to appear before court, e.g. because they are going abroad³⁸. It is worth emphasising that the police can do things that are in the scope of their competence and that a victim cannot do. In case the injured party, i.e. a victim, decides to file a complaint directly to the police, whatever action of a prosecutor is excluded from the activities aimed at detecting a perpetrator of a crime pursued based on a private accusation. A prosecutor may join in if he finds social interest in his interference. The essence of this proceeding is the lack of whatever type of a prosecutor's participation. If it were assumed that a prosecutor could take any steps in this proceeding (e.g. issue a decision on a search or release from official secrecy), it would have to be connected with his recognition of a social interest in this kind of intervention. Even a single act like this would express that there are prerequisites of his interference. This would change the proceeding into *ex officio* one and would go beyond the scope of the proceeding.

Accepting a prosecutor's interference would lead to a situation, in which a proceeding intended to be fast and not formalised would become a real proceeding restricted only by the statute of limitation, in which almost every activity might be performed³⁹. From this perspective, not only a victim but also the police, after a complaint has been filed in the discussed mode, have no procedural possibilities of obtaining the communications traffic data (a billing), and as a result determining personal data of an internaut who uses a modem and a telephone protected by the communication secrecy. Only a prosecutor may exempt someone from that secrecy, but his participation is excluded from the proceeding and he cannot perform any activities in it. It must be stated that an IP address, an email address, a number of instant messaging program and a number of the telecommunications subscriber in case of a connection to the Internet through a modem are data that may be really useful evidence in the criminal proceeding, which – in case of this kind of proceeding – due to their specificity, in most cases are practically the only way leading the identification of a perpetrator. The establishment of the subscriber's station number or the identification of a server from which a connection was initiated or a message was sent is not always sufficient to identify a person making a connection and it does not prejudge the true address of the sender of a message emailed. There are unlimited ways of manipulating the data in the header fields and the impersonating techniques in electronic mail are commonly known⁴⁰.

³⁸ R.A. Stefański, *Kodeks postępowania karnego. Komentarz* [Criminal Procedure Code – Commentary], Warszawa 2004, p. 403.

³⁹ T. Fołta, A. Mucha, *Zniesławienie i znieważenie...* [Defamation and insult...], *op. cit.*, p. 59.

⁴⁰ P. Bocij, *Cyberstalking: harassment...*, *op. cit.*

The use of the so-called anonymous email programs available on the web that delete the original address from the message header makes it possible to remain totally anonymous. In some situations it is necessary to match other evidence to identify a perpetrator. A method of obtaining other evidence may be a search of venues and a seizure of computers or data storage devices in order to read the disc memory data⁴¹. Problems with the identification of a stalker may also occur in case a computer system is composed of many workstations, servers and devices used for archiving data, e.g. in case of business activities, or when they are in places where many people use computers connected to the Internet. Quite often, in complex corporate networks where a big number of computers are connected, the most frequent method of ensuring data security is separating the internal computer network from the web with the use of a firewall. It is a computer with an IP address recognisable outside and all the communication between the computers protected this way with the web takes place via a proxy server. A direct result of this configuration is both inability to unauthorised access to the internal network and the lack of detailed information in the server's logfiles about the IP address of the computer a cyberstalker used, e.g. entering a defaming content on a forum. This is because the IP address of the firewall server will only be registered in the logs⁴². If a company employee or a user of the network hidden behind a firewall wants to connect to the Internet website, the server of that website registering the IP address of the computer connecting with it is going to register the IP of the proxy and not a computer of an employee or a user. The true address will remain unrevealed. In each such case, all the computers under the proxy server should be examined. The seizure of many computers, although technically possible, violates the principle of proportionality and the examination of their contents is costly and time consuming. Copying the contents of a hard disc for further forensic examination is an alternative to a computer seizure. It is worth remembering that the operating system logfile identifying a computer IP address does not constitute evidence if it had been used by an anonymous cyberstalker as an intermediary to an unlawful activity, which makes the detection of a perpetrator even more difficult. The Criminal Procedure Code restricts the decision on the seizure of things and a search to a court or a prosecutor's competence and allows only for indispensable activities by the police or another agency in urgent cases.

A stalker may be aggressive at the beginning or after some time of harassing a victim. The situation may develop gradually, sometimes with intervals; sometimes a victim may succeed in liberating from stalking, which depends on various circumstances and personality features. Stalking may also result in other

⁴¹ A. Adamski, *Prawo karne komputerowe* [Criminal computer law], Wyd. C.H. Beck, Warszawa 2000, p. 198.

⁴² T. Folta, A. Mucha, *Zniesławienie i znieważenie...* [Defamation and insult...], *op. cit.*, p. 61.

crimes as a burglary, an injury, a rape and even a murder. That is why victims' fears must be treated seriously as this may be an introduction to a serious crime. It is important that a perpetrator seeks contact with victims against their will and attempts to do that with great determination. In many situations his aim is to have a sexual intercourse or a love affair with a victim. Some stalkers, including cyberstalkers, derive satisfaction from the fact that they have influence on a victim's life, may control it, evoke fear by appearing suddenly etc. Their motivation may evolve and trying to win a victim's favour faced with a rejection may change into threats and severe forms of harassment⁴³.

Intensity and long-lasting nature of activities are typical of a stalker's conduct. Intensity may occur as multiple calls at night, waiting in front of a victim's house every day for hours, repeated puncturing of car tyres, visiting a victim at workplace regularly etc. It was established that harassment of victims in the USA takes from four weeks to eight years (an average of 1.75 years); there was a case in which it took 20 years. Stalkers are sophisticated in pursuing their goals, really inventive and having all kinds of manipulations ready. This is why it is difficult to predict their behaviour although their aim to have contact with a victim shows a high level of perseverance. A sample of 74 stalkers registered by the Police in Los Angeles was divided into three sub-groups: (1) people suffering from erotomania with delusion disorder who have no relationship with a victim, (2) people suffering from obsessional love with psychic disorder (and erotomania) who have no relationship with a victim either, and (3) people with an obsession who have contacts with a victim⁴⁴. Only seven persons (10%) were classified as erotomaniacs and 35 persons (47%) were classified as ordinary obsessional stalkers having contact with their victims. Psychotic symptoms that stalking is often connected with, and that are most important from court and clinical perspective are, apart from erotomaniac ones, delusions based on jealousy. The number of perpetrators with jealousy-related disorder ranges from non-psychotic morbid jealousy to delusional jealousy and the state is believed to be quite common stalkers' motivation.

The relationship between jealousy, psychosis and severe acts of violence was described in psychological literature. Inter alia, 46 delusional jealousy-related murder perpetrators were examined⁴⁵. It turned out that 20 of them followed their spouses before the assault. Other research confirmed that most victims had been followed or spied on by the assaulters. 30% of perpetrators vandalised their victims' property. Delusional jealousy is also strengthened by psychotic and non-psychotic symptoms as well as environmental factors that can play an important

⁴³ S. Furnell, *Cybercrime: vandalizing the information society*, Addison Wesley, London 2002.

⁴⁴ M. Zona, K. Sharma, J. Lane, *A comparative study of erotomaniac and obsessional subjects in a forensic sample*, *Journal of Forensic Sciences* 1993, 38, pp. 894–903.

⁴⁵ R.R. Mowat, *Morbid jealousy and murder: A psychiatric study of morbidly jealous murders at Broadmoor*, Tavistock, London 1966.

role in perpetrator's behaviour⁴⁶. Long before committing the crime of stalking, future perpetrators demonstrated the behaviour consisting in controlling and insulting their partners⁴⁷. Former partners who committed stalking, more often than others, demonstrated the following behaviour: they found it difficult to look at things from the partner's point of view (87.7% of partners versus 57.8% of spouses); they tried to provoke quarrels (83% vs. 45.3%); they were jealous or possessive (83.7% vs. 46.3%); they tried to limit their victims' contact with family and friends (77.1% vs. 32.2%); they insisted to know where their partners were all the time (80.7% vs. 34.4%); they felt underestimated (85.5% vs. 40.9%); they shouted at their partners or insulted them (88.5% vs. 44.5%); and they threatened their victims (92.2% vs. 33.1%).

A term "obsessional harassment" was proposed to refer to the key characteristics of stalking⁴⁸. There were three reasons for that: (1) to support clinical examinations with the use of a clearly defined label, free of sensation; (2) to identify the most commonly occurring unlawful acts committed by stalkers; and (3) to explain obsession, which is an important cognitive and motivational component of stalking. An obsessional stalker is a person getting involved in abnormal or long-term harassment or threatening of a given person. A review of research into the issue of obsessional harassment by almost 200 perpetrators recorded by the police was conducted⁴⁹. Obsessional stalkers demonstrated a much lower level of anti-social personality disorder than other convicts. A hypothesis was formulated that such people develop "narcissistic fantasies" linking them with objects, which is typical of exclusion from the real world and leads to shame and humiliation. They demonstrated various types of anti-social behaviour. The research confirmed earlier hypotheses that the people had had unsuccessful heterosexual relations for at least ten years before aberrational behaviour occurred. Perpetrators often abuse drugs and get addicted, and often show state of mind disorder. The occurrence of anti-social personality disorder established in earlier research was also confirmed.

There are hypotheses that stalking is connected with the styles of attachment people develop based on childhood experience. Healthy relations based on appropriate attachment do not cause inappropriate behaviour or actions in adult life. People with narcissistic and borderline types of personality are more likely to become stalkers because they get irritated easily⁵⁰. At the same time, it is

⁴⁶ R. Tjaden, N. Thoennes, *Stalking in America: Findings from National Violence Survey*, National Institute of Justice, Washington 1998.

⁴⁷ N.S. Jacobson, J.M. Gottman, *Violent relationship*, *Psychology Today* 1998, no. 3–4, pp. 60–65.

⁴⁸ J.R. Meloy, S. Gothard, *Demographic and clinical comparison of obsessional followers and offenders with mental disorders*, *American Journal of Psychiatry* 1995, 152, pp. 258–263.

⁴⁹ J.R. Meloy, *Stalking (obsessional following). A review of some preliminary studies*, *Aggression and Violence Behavior* 1996, no. 1, pp. 147–162.

⁵⁰ W. Petheric, *Cyberstalking: obsessional pursuit and digital criminal*, http://www.trutv.com/library/crime/criminal_mind/psychology/cyberstalking/3.html (10.12.2013).

highlighted that in case of stalking, one cannot speak of psychopathologies but only about personality types. As a result, nobody has described a personality profile of a typical stalker yet. The analysis of primary differentiation (making a nuisance in general) shows that such behaviour may be defined as stalking if it is intentional, occurs for at least thirty days and results in boundless fear. Analysis of secondary differentiation makes it possible to define stalking as a phenomenon that causes consequences in the psyche and relations with others (anxiety, sleep disorder, necessity of changing a telephone, work or place of residence) and “involves” the next of kin, family, friends, acquaintances and colleagues.

The analysis of a perpetrator’s activities makes it possible to select a few types of stalkers’ personality (psychological profiles). There are such types as: a rejected stalker – who harasses his victims in order to change or improve the state of rejection, e.g. as a result of divorce, separation or the end of a relationship with a partner; a resentful stalker – who harasses victims because of the feeling of harm, resentment and bitterness to a victim; he wants to induce fear and make a victim suffer; an intimacy seeker – who seeks close contact with a victim, wants to develop an intimate, close and loving relation with a victim who is, in his view, a long searched for kindred spirit and is convinced that it was their destiny to meet and be together; an incompetent suitor – who, despite poor social skills and in making advances to women, has an obsession or entitlement to develop an intimate relation with a victim who attracted his love interest; a predatory stalker – who spies on a victim in order to prepare a plan of a sexual assault; a simple obsessional stalker – who had a personal, close relationship with a victim before; although they had a short-term contact, e.g. a ‘blind date’, he acquires an obsessional conviction that he will be either with a person who does not want him or with nobody else; erotomaniac – who is convinced that a victim is fascinated with him and loves him, and even if the other person recedes, it is because of strong affection to him; a love obsessional stalker – who develops a love obsession to a victim and knows that the other person does not love him; most often such perpetrators suffer from a mental disorder, e.g. schizophrenia or mania and even try to combat the problem⁵¹. According to the National Organisation for Ending Violence Against Women, every stalker’s activity resulting in a victim’s feeling of fear and horror, and lost security belongs to the catalogue of stalking activities – conscious and malicious harassment of the beloved.

⁵¹ J. Kosińska, *Prawnokarna problematyka stalkingu* [Legal-penal issue of stalking], Prokuratura i Prawo 2008, no. 10, pp. 45–46.

4. Stalkers' motives behind their activities

Stalking may be classified with the use of various criteria, e.g. taking into account stalkers' motives and psyche or the relationship between a perpetrator and a victim⁵². The following types of relationship are distinguished:

1. Victims having a close relationship with a perpetrator in the past. The contacts they had initiated obsessional behaviour in a stalker's psyche. They are mainly former partners or participants of sexual scandals but also a patient-doctor relationship.
2. A victim comes from a stalker's broader social circle or had an accidental contact with a perpetrator. For example, a man meets a woman he has not known in his company yet and since that moment he complements her in the mistaken belief that they are meant for each other.
3. A victim is a public person who thanks to a medial image becomes a stalker's target.

Research into stalking and cyberstalking was also conducted among university students and with respect to children and youth. The research took into account both perpetrators' and victims' features and types of stalking in a sample of 13 persons in the age of 9–18⁵³. The research results confirmed many findings concerning adults, including those that most young stalkers are males, most victims are females and about half of all stalking cases included threats towards victims. The share of cases with the use of violence was about 31%, the most common methods used by perpetrators were: physical contacts, letter writing and telephone calls. An examination of files carried out in a court in Massachusetts showed that 757 restrictive orders were issued in the period of only ten months towards young criminals in cases of threats, stalking and harassment. Other research into sexual harassment in American schools conducted by the American Association of University Women provides proofs that also schools are not free from stalking. Among 81% of students reporting sexual harassment at school, 7% were spied on, 37% were victims of gossiping and 23% avoided venues where they had been harassed⁵⁴. Cyberstalking plays more and more important role in all the harassment activities⁵⁵. Research may provide important information on factors preceding the occurrence of inappropriate behaviour and may facilitate early detection, combating, prevention and decreasing the risk. The research conducted so far made it possible to establish many victims' features and victim-

⁵² B. Hołyst, *Psychologia kryminalistyczna* [Forensic psychology], Wyd. Prawnicze LexisNexis, Warszawa 2004, p. 636.

⁵³ J.T. Mc Cann, *Subtypes of stalking (obsessional following) in adolescents*, *Journal of Adolescence* 1998, 21, pp. 667–675.

⁵⁴ American Association of University Women, *Hostile hallways: the AAUW Survey on sexual harassment in American schools*, Washington DC, 1999.

⁵⁵ S. Kozak, *Patologie komunikowania w Internecie* [Pathologies of communicating on the Internet], Wyd. Difin, 2011, pp. 207–212.

perpetrator interactions. Research into a bigger sample would make it possible to establish differences between the psychosexual development of adolescents and adults and formulate hypotheses concerning young stalkers' behaviour when they become adults.

5. Stalking prevention

For over ten years in the USA, there have been attempts to have control over stalking with the use of special forms of crisis management. In 1990, a special operational group of officers was established, which at first specialised in the protection of stars and then also ordinary citizens against stalking. The officers of Los Angeles Threat Management Unit cooperate with the scientists in the field of social sciences⁵⁶. Efficient fight against stalking and its prevention require forensic, psychological and legal actions. Prevention is mainly to minimise the areas of assaults committed by obsessional fans. That is why the first step is the protection of anonymity of workplace and privacy in order to decrease the attractiveness of a person in the eyes of a perpetrator. It can be achieved, inter alia, by planning a certain way of presenting a prominent person in the media and specific strategies concerning contacts with fans. As celebrities receive a lot of emails, a special correspondence filtering programs should be installed to select email letters. In the first stage of correspondence analysis, special checklists are used to review the incoming mail. They should take into consideration special features of a vulnerable group, e.g. the fact that entertainment industry celebrities are sent love letters, and politicians – complaints and requests for help as well as letters with various political opinions of their authors. An example of a risk factor is the author's identification with a well-known criminal. There was a cyberstalking case in which a man with a sexual murderer personality harassed a woman. In the second stage of the analysis, it is recommended to thoroughly examine the motives behind the activities, personal features and possible alternative activities of a perpetrator. The motive behind a violent act may be a wish to draw the attention of the admired prominent person.

The victims of stalking, including cyberstalking, most often seek protection in the legal system, but legal measures, including court orders and police warnings, prove to be inefficient because perpetrators often ignore them. It was also established that the perpetrators who had demonstrated negative emotions and used violence when the obsessional tendencies intensified, posed the highest risk of committing acts of aggression towards their victims. The hypothesis of higher probability of acts of aggression on their part was also confirmed by the research

⁵⁶ L. McFarlane, P. Bocij, *An exploration of predatory behavior in cyberspace: Towards a typology of cyberstalkers*, <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1076/996> (1.09.2003).

conducted by P. Mullen, M. Pathe, R. Purcell and G. Stuart⁵⁷. The discussed research made it possible to draw many conclusions concerning stalkers, inter alia, that:

- stalkers do not constitute a uniform group and only personal features of a given person may be important for the assessment of possible aggressive behaviour;
- victims' strategy most often consists in seeking legal assistance; ignoring stalkers is more common among young, courageous victims;
- 1/3 of victims decided to be confronted with stalkers but the method resulted in intensification of harassment rather than giving it up;
- although most stalkers use threats towards victims, this does not mean that they will be fulfilled. Similarly, indication of perpetrators' mental or personality disorder does not constitute the forecast of the use of violence by stalkers.

Unlike in cases of harassment in real world, cyberstalking leaves many more traces that can constitute grounds for conviction. Keeping logfiles by victims, an archive of messages, emails and short text messages, and billings confirming persistent attempts to have contact make it possible to establish guilt quickly and apply one of the above-mentioned regulations. Tips recommending that victims collect proofs of stalking are really valuable. They should record facts concerning venues and time of harassment, witnesses of these events, store texts and recordings on data collection devices, facsimiles, letters, emails etc.⁵⁸ There are also other possibilities of protecting against cyberstalking, e.g. by searching messages with particular content sent to particular people. It is very important to be careful when exchanging information via the Internet. As it was mentioned earlier, a stalker leaves an "electronic trail" on the Internet, but detecting it requires adequate police training. However, the most important thing for efficient prosecution is the development of good legal grounds. The information obtained in recent years indicates that it is possible to deal with stalking in a professional way and achieve good results in combating this crime. It is certainly necessary to continue research into this issue. The acquired knowledge should also be used in these countries where the phenomenon of stalking did not use to be classified as a crime. It is also essential that well designed law regulate such an important sphere of interpersonal relations as communication in cyberspace, where millions of people contact each other using their genuine names and other personal data.

It is especially important to find an answer to the question how the threat of becoming a victim of cyberstalking can be prevented or eliminated. The question is especially important in case when an indefinite threat lurks around a potential victim and a perpetrator appears suddenly and disappears. One cannot forget that

⁵⁷ P. Mullen, M. Pathe, R. Purcell, G. Stuart, *A study of stalkers*, American Journal of Psychiatry 1999, 156, pp. 1244–1249.

⁵⁸ G.E. Wattendorf, *Stalking – investigating strategies*, FBI Law Enforcement Bulletin, March 2000, pp. 10–14.

one's own activities ensure, apart from increasing security, many psychological advantages, at least the reduction of the feeling of helplessness. Many activities against cyberstalking refer to the increased protection of the so-called sensitive data: keeping an address, a telephone number etc. secret⁵⁹. It is emphasised that it is essential to collect facts that are important for court and documenting the occurrences of stalking and their details: time, venues, witnesses, messages on telephones (voice mail), facsimiles, letters, emails etc.

CYBERSTALKING AS A FORM OF CYBERHARASSMENT

Summary

The phenomenon of cyberstalking refers to the use of the Internet or other means of electronic communication in order to harass a person, a group of people or an organisation. It can cover a wide range of various types of activities having adverse effect on victims and harming them. Cyberstalking constitutes a form of stalking. Dangers that this form of violence carries were noticed for the first time in the USA in the early 1990, which resulted in the development of state and federal provisions regulating a series of a perpetrator's activities. Behaviour that is called cyberstalking relates to many different activities. They include, inter alia, false accusations aimed at ruining a victim's good name. These accusations are often published in various places on the web, such as blogs, social networking sites etc. Cyberstalkers collect different information about their victims and their families, friends, the surrounding etc. They search for this information on the Internet and sometimes hire specialists, e.g. private detectives. They monitor the behaviour of their victims on the web in real time (online), often attempt to steal their personal passwords and this way get access to personal information⁶⁰. One of the manifestations of cyberstalking is encouraging other people to harm a victim – to this end, stalkers present a victim as a person guilty of many evil deeds, display a victim's personal data, photographs, address, telephone number etc. Cyberstalkers often present a victim as a person harassing them. Sometimes cyberstalking is expressed through infecting a victim's computer with viruses, and sometimes ordering – on a victim's behalf – various goods, such as erotic gadgets or pornographic magazines subscriptions, which are then delivered to a victim's house. In case of young people, cyberstalkers often seek to arrange real-life meetings with them.

⁵⁹ P. Bocij, *Cyberstalking: harassment in the Internet age and how to protect your family*, Praeger Press, Westport C.T., 2004.

⁶⁰ *Ibid.*, pp. 9–10.

CYBERSTALKING JAKO FORMA CYBERPRZEMOCY

Streszczenie

Zjawiskiem cyberstalkingu określa się wykorzystywanie Internetu lub innych środków komunikacji elektronicznej w celu nękania jednostki, grupy osób lub organizacji. Może obejmować szeroką gamę różnego rodzaju działań niekorzystnych dla ofiary i szkodzących jej. Cyberstalking stanowi jedną z form stalkingu. Niebezpieczeństwa, jakie niesie ze sobą ta forma przemocy, zostały dostrzeżone po raz pierwszy na początku lat dziewięćdziesiątych ubiegłego wieku w USA, w efekcie czego ciąg zachowań sprawcy został tam uregulowany zarówno w przepisach stanowych, jak i regulacjach federalnych. Zachowania określane mianem cyberstalkingu obejmują wiele specyficznych czynności. Należą do nich m.in. fałszywe oskarżenia, których celem jest zniszczenie dobrego imienia ofiary. Oskarżenia te bardzo często publikowane są w różnych miejscach sieci, takich jak blogi, serwisy społecznościowe itp. Cyberstalkerzy zbierają różnorodne informacje o swoich ofiarach, ich rodzinach, znajomych, otoczeniu itp. Poszukują tych informacji w Internecie, a niekiedy wynajmują w tym celu specjalne osoby, np. prywatnych detektywów. Sprawcy monitorują zachowania swoich ofiar w sieci na bieżąco (online), próbują często odkryć ich osobiste kody i w ten sposób zyskać dostęp do bardzo osobistych informacji. Jednym z przejawów cyberstalkingu jest zachęcanie innych osób do wyrządzania krzywdy ofierze – w tym celu przedstawia się ofiarę jako osobę winną wielu różnych negatywnych działań, prezentuje jej dane osobowe, fotografie, adres, numer telefonu itp. Bardzo często cyberstalkerzy przedstawiają ofiarę jako prześladowcę ich samych. Cyberstalking wyraża się niekiedy w zarażaniu oprogramowania komputerowego ofiary wirusami, a czasami w zamawianiu – rzekomo w imieniu ofiary – różnych dóbr, takich jak gadzety erotyczne, czy subskrybowanie pism pornograficznych, które są potem dostarczane do mieszkania ofiary. W przypadku ludzi młodych, cyberstalkerzy dążą często do aranżowania z nimi spotkań w świecie realnym.

L' HARCÈLEMENT ÉLECTRONIQUE EN TANT QUE LA FORME DU CYBER-VIOLENCE

Résumé

Le phénomène de l'harcèlement électronique est défini par emploi de l'Internet ou d'autres moyens de communication électronique afin d'oppresser un individu, un groupe de personnes ou une organisation. Il peut comprendre une large gamme de différentes actions difficiles pour la victime et nuisibles pour elle. L'harcèlement électronique est une des formes de l'harcèlement. Les dangers suivis par cette forme

d'oppression ont été remarqués pour la première fois au début des années 90 du siècle passé aux Etats Unis et en effet, la suite du comportement de l'actant y a été réglée aussi bien dans les droits d'états que dans les règlements fédéraux. Le comportement défini par le nom d'harcèlement électronique comprend plusieurs activités spécifiques. Y appartient entre autre les accusations fausses afin de détruire le bon nom de la victime. Ces accusations sont très souvent publiées dans les places différentes en ligne, comme par exemple les blogues, les réseaux sociaux etc. Les harceleurs électroniques ramassent les informations différentes sur leurs victimes, leurs familles, connaissances, entourage, etc. Ils cherchent ces informations à l'Internet et parfois même louent à ces fins des personnes spéciales, par exemple les détectives privés. Les exécuteurs suivent le comportement de leurs victimes en ligne, ils essaient souvent de découvrir leurs mots de passe personnels pour avoir accès aux informations très personnelles. L'un des exemples d'harcèlement électronique est l'invitation des autres pour faire des outrages à la victime – et pour acquérir ce but on présente la victime comme une personne qui a commis plusieurs actes négatifs, on publie ses données personnelles, les photos, l'adresse, les numéros de téléphone etc. Très souvent les harceleurs électroniques présentent la victime comme un oppresseur d'eux-mêmes. L'harcèlement électronique s'exprime parfois par la contamination du hardware de l'ordinateur de victime par le virus, ou parfois par commander – au nom de la victime soi-disant – de différents biens comme par exemple les gadgets érotiques ou l'abonnement de la presse pornographique qui sont livrés à domicile de la victime. Au cas des jeunes gens les harceleurs électroniques mènent très souvent à arranger leurs rencontres dans le monde réel.

КИБЕРСТАЛКИНГ КАК ФОРМА КИБЕРНАСИЛИЯ

Резюме

Явление киберсталкинга связано с использованием Интернета или других средств электронной коммуникации с целью преследования отдельного лица, группы лиц либо организации. Может охватывать широкую гамму разнообразных действий, нежелательных для жертвы и причиняющих ей вред. Киберсталкинг представляет собой одну из форм сталкинга. Опасности, вызываемые данной формой насилия, были замечены впервые в начале девяностых годов прошлого столетия в США, в результате чего ряд действий преступника был урегулирован как в положениях отдельных штатов, так и федеральных законах. Тип поведения, определяемый как киберсталкинг, предполагает совершение множества специфических действий. К ним относятся, в частности, ложные обвинения, целью которых является нанесение урона доброму имени жертвы. Подобные обвинения часто публикуются в различных сетевых локализациях, таких, как блоги, социальные сети и т.п. Киберсталкеры

собирают разнообразную информацию о своих жертвах, их семьях, знакомых, окружении и т.п. Ищут эту информацию в Интернете, а нередко нанимают для этой цели специальных людей, например, частных детективов. Преступники круглосуточно наблюдают за поведением своих жертв в сети (online), часто взломать их коды и тем самым получить доступ к сугубо личной информации. Одним из проявлений киберсталкинга является побуждение третьих лиц к нанесению вреда жертве как лицу, которому вменяется вина в виде совершения различных негативных поступков, представление её личных данных, презентация фотографий, адреса, номера телефона и др. Довольно часто киберсталкеры представляют свою жертву как своего же преследователя. Киберсталкинг нередко проявляется в заражении компьютерного программирования жертвы вирусами, иногда в реализации заказов – якобы от имени жертвы – различных товаров и услуг, таких, как эротические гаджеты, или подписка на порнографические журналы, которые затем доставляются по месту жительства жертвы. Если речь идёт о молодых людях, киберсталкеры часто стремятся к организации встреч в реальной действительности.