EFFECTIVE LAW IN AN EFFECTIVE STATE

Local conditions in the global context in the face of 21st century challenges of fighting crime.

CYBER VIOLENCE AGAINST WOMEN

Author of the analysis: Kamila Groszkowska

The analysis was prepared as part of the project:
Effective law in an effective state. Local conditions in the global context, in the face of 21st century challenges of fighting crime

Financed by the Justice Fund administered by the Minister of Justice

Translated by: Agnieszka Janczak

FUNDACJA INSTYTUT PRAWA USTROJOWEGO

www.ipu.org.pl
https://efektywne-prawo.org.pl/

https://www.facebook.com/fundacjaipu

fundacja@ipu.org.pl

MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl

INSTYTUT PRAWA USTROJOWEGO

FUNDUSZ SPRAWIEDLIWOŚCI

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości"

Table of Contents

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości”

Introduction

Violence against women on the Internet is a relatively new phenomenon, related to the dynamic technological development, as well as more and more widespread access to the Internet and social media.

Cyber violence is not defined in the Polish law or international law instruments. It includes many behaviours and forms of violence committed on the Internet or with the use of communication technology. Cyber violence experienced by women should be understood as a form of gender-based violence rooted in systemic inequalities between men and women. It poses a real threat to women all over the world, and the most vulnerable group are girls and young women up to the age of 29. The most common forms of cyber violence are bullying, intimidation and sexual harassment, however, it can also take the form of economic violence or lead to physical violence. The scale of the phenomenon is difficult to estimate due to the small amount of research, low reporting rate, low detection rate as well as educational deficiencies in society. Violence against women on the Internet is often underestimated due to the general consent to sexism in the virtual space and perceiving it as a phenomenon of low social harmfulness[1].

Cyber violence is a global problem and can have serious social and economic consequences[2]. It is related to the increasing network access. In 1995, less than 1% of the world's population had access to the Internet[3]. After 25 years, this number increased to approx. 59%, which now gives over 4.5 billion users[4]. Over 4 billion are active users of social media, where cyberbullying is the most common. By 2030, the number of active Internet users is projected to increase to 7.5 billion and cover 95% of the world's population[5]. According to 2015 data from UN Women, as many as 73% of women worldwide have experienced some form of cyberbullying at least once in their lives. With such a dynamic increase in Internet users, one can expect a proportional increase and intensity of cyberbullying. Providing universal and affordable access to the Internet as a condition of economic prosperity has been

[1] Z. Warso, J. Smętek, *Cyberprzemoc wobec kobiet. Raport*, Helsinki Foundation for Human Rights, Warszawa 2017, [available at:] https://www.hfhr.pl/wp-content/uploads/2017/12/HFPC-Cyberprzemoc-wobec-kobiet-raport-www.pdf.
[2] European Institute for Gender Equality, *Cyber violence against women and girls*, 2017.
[3] UN Broadband Commission For Digital Development Working Group On Broadband And Gender, *Cyber violence against women and girls a world-wide wake-up call*, p. 2, [available at:] https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?vs=4259.
[4] Global digital population as of October 2020, Statista, https://www.statista.com/statistics/617136/digital-population-worldwide, (accessed on 20.12.2020).
[5] S. Morgan, Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion, https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/] (accessed on 20.12.2020).

identified as one of the actions under the UN Sustainable Development Goal 9[6]. In this context, it is particularly important to ensure that the virtual space is a safe place for girls and women.

[6] Sustainable Development Goals UN, Goal 9, Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation, https://sdgs.un.org/goals/goal9, [accessed on 20.12.2020].

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości"

Definition and forms of cyber violence

The concept of violence against women on the Internet, or cyberbullying, has not been defined in the instruments of international law, European law or Polish law. Pursuant to the Council of Europe Convention on preventing and combating violence against women and domestic violence[7] (hereinafter: the Istanbul Convention) violence against women is understood as a violation of human rights, a form of discrimination against women and includes any act of gender-based violence that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether in public or in private life. Consequently, the conceptual scope of the concept of cyberbullying against women covers all such acts of violence, committed, assisted or exacerbated by the use of communication technology, i.e. mobile phones, the Internet, social media, online computer games, text messages and others[8]. Cyberbullying may take the form of intimidation, sending unsolicited sexual content, or publishing private information[9]. It is possible to become a victim of online violence regardless of gender or age, but the available research shows that it affects women and girls much more often[10]. According to data published by the *Working to halt Online Abuse* organization, between 2000 and 2013, 70% of the analysed cases were female victims, of which 42% were between 18 and 30 years of age[11]. Women and girls are particularly vulnerable to various forms of sexual cyberbullying, such as threats of rape, sending pornographic content without consent, harassment, unwanted sexual advances, attacking and insulting women in relation to their sexuality, publicizing information about their intimate life[12]. It is worth emphasizing that violence on the Internet should not be seen as a less serious phenomenon, detached from the real world, but rather as real violence that occurs through the use of technological means[13].

Cyber violence against women is a form of gender-based discrimination and an expression of systemic inequalities between women and men[14]. In the Istanbul Convention, violence against women

[7] Council of Europe Convention on preventing and combating violence against women and domestic violence signed in Istanbul on 11 May 2011, Journal of Laws of 2015 item 961.
[8] UN Women, Types of violence against women and girls, https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/types-of-violence, [accessed on 20.12.2020].
[9] Ibidem.
[10] See Z. Warso, J. Smętek, *Cyberprzemoc*..., op. cit.
[11] Working to Halt Online Abuse, Comparison Statistics 2003-2013, http://www.haltabuse.org/resources/stats/Cumulative2000-2013.pdf.
[12] Z. Warso, J. Smętek, *Cyberprzemoc*..., op. cit.
[13] EIGE Europa, Cyber violence against women, https://eige.europa.eu/gender-based-violence/cyber-violence-against-women, [accessed on 20.12.2020]
[14] Ibidem.

has been recognized as one of the basic social mechanisms wherein women are seen as subordinate to men and a consequence of the historical domination of men over women. This mechanism is also noticeable when it comes to violence on the Internet. Most often it takes the form of sexual or psychological abuse, but it can also have the hallmarks of economic violence, e.g. when publishing certain information on the Internet exerts a negative impact on the victim's employment status[15].

Online violence can take many forms and escapes a uniform classification. One of the most common types of it is cyberstalking, understood as persistent and unwanted harassment by means of communication technology that disturbs the victim's sense of security and induces anxiety or fear[16]. Cyberstalking may involve sending text messages, e-mails, instant messages that contain threats or offensive content, posting comments or content offensive to the victim on the Internet, sharing victim's private photos or videos or content that allows them to be identified. Another form of stalking is the use of technology (such as GPS) to track the victim or monitor their internet activity[17]. A characteristic feature of cyberstalking is repetitiveness of an action committed by the same person. One type of cyberstalking is harassment. Unlike stalking, harassment does not necessarily involve fear of being hurt by the perpetrator. It rather takes the form of publishing private information about the victim, such as their address, telephone number, information about their finances, about family members, obtained, most frequently, through doxing[18]. Another form of harassment is swatting, i.e. making false reports to the police about crimes committed in the places where the victim is, in order to send police units there[19].

The second common type of cyberbullying is sexual harassment or exploitation on the Internet. It includes activities such as sending unsolicited messages with sexual content, making offensive and unwanted proposals via social networks or chat rooms, threats of physical or sexual violence in private messages or comments posted on the Internet, and the use of gender-based or sexuality-based hate speech[20]. A special type of abuse is the dissemination of erotic or pornographic materials without the consent of the person whose image appears in these materials. It can take the form of the so-called revenge porn, where the perpetrator is a former partner who is in possession of erotic materials and content from the relationship times or other persons who try to humiliate the victim and cause real

[15] European Institute for Gender Equality, *Cyber…* op. cit.
[16] Ibidem, p. 4.
[17] UN Broadband Commission For Digital Development Working Group On Broadband And Gender, *Cyber violence…* op. cit., p. 22.
[18] Women's Media Center, Online Abuse 101, https://www.womensmediacenter.com/speech-project/online-abuse-101/#doxing, [accessed on 20.12.2020].
[19] Ibidem.
[20] European Institute for Gender Equality, *Cyber…*op. cit.

damage to their life[21]. Erotic materials may be obtained from the victim with their consent, by force or illegally without their knowledge and consent, e.g. by hacking the victim's phone, computer, or social media accounts. Another form of sexual cyberbullying is the so-called sextortion, a form of online blackmail that involves demanding the delivery of photos, videos of an erotic nature, or demanding sexual acts from the victim under threat of harm or making their private or intimate content public[22].

Due to the dynamic technological development, women are exposed to new forms of cyberbullying. They include among others putting financial pressure on the Internet by denying access to online accounts, manipulating credit information or stealing identity. Another threat is the so-called google bombing, consisting in the intensive flooding of the search engine with external links that are to quickly affect the positioning of a given expression or phrase[23]. In consequence, it is possible, for example, to associate the offensive phrase entered in an Internet search engine with the name of a given person, in order to humiliate or ridicule them. This is especially severe and dangerous for women holding public offices. Cyberbullying can also be used for criminal activities, such as human trafficking.

[21] Ibidem.
[22] L. Blanch, W. L. Hsu, *An Introduction to Violent Crime on the Internet* [in:] Cyber Misbehavior, Vol. 64, No 3, 2016.
[23] Delante, Google Bomb, https://delante.pl/definicje/google-bomb/, [accessed on 20.12.2020].

Cyber violence in the Polish law

Cyber violence has not been defined in the Polish law or regulated in a single legal act. Depending on its form, victims can claim their rights under the provisions of criminal law, civil law or even labour law. As a party to the Istanbul Convention, Poland is obliged under Art. 4 to adopt legislative and other measures to protect the rights of all, and of women in particular, to live free from violence in the public and private spheres. Art. 34 of the Istanbul Convention stipulates an obligation to criminalize harassment, that is, deliberately repeated intimidating actions directed against a person, causing them to fear for their safety. Art. 40 of the Istanbul Convention obliges parties to penalize sexual harassment, understood as sexual images or undesirable sexual verbal, non-verbal or physical acts that violate the dignity of a person, in particular in an intimidating, hostile, degrading or humiliating atmosphere. The call for the parties to the Istanbul Convention to take action to counteract cyberbullying also results from Art. 17 of the Convention. According to this article, the parties are to encourage the private sector, the information and communication technology sector and the mass media, respecting freedom of expression and their independence, to participate in the development and implementation of appropriate strategies, as well as setting guidelines and internal standards to prevent violence against women and promote respect for their dignity. In addition, the parties will develop, in cooperation with the private sector, and promote among children, parents and educators, the skills to safely move in an information and communication environment that allows access to degrading sexual or violent content that may be harmful.

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości”

Cyber violence in the criminal law

The forms of cyberbullying penalized in Polish criminal law can be divided into three groups of crimes: crimes related to harassment, threats, insults, hate speech; crimes related to the sexual sphere, including abuse, dissemination of pornographic content; crimes of identity and data theft, obstruction of access to information.

One of the most common forms of cyberbullying against women is cyberstalking, i.e. persistent harassment. The term was introduced to the Penal Code in 2011[24] and specified in Art. 190a thereof. Pursuant to Art. 190a §1 of the Penal Code: anyone who by persistent harassment of another person or their closest environment induces justified by the circumstances sense of threat, humiliation or torment, or significantly violates their privacy, is subject to imprisonment from 6 months to 8 years[25]. The protected value is freedom from fear and freedom from any form of tormenting, humiliation or harassment, i.e. the broadly understood psychological freedom of a human being[26]. Harassment means repetitive, multiple acts, legal or illegal, the purpose of which is to torment, annoy, or disturb the victim or their closest family[27]. Art. 190a criminalizes persistent harassment. In the judicial practice, persistent harassment is defined as unyielding behaviour, when the perpetrator continues the harassment for a longer period of time despite requests and reprimands from the victim or other persons[28]. The perpetrator's behaviour must result in creating a justified sense of threat or a sense of a significant breach of privacy in the aggrieved party. To assess the justified sense of threat, both subjective criteria, i.e. the victim's internal feelings, and objective criteria, indicating circumstances justifying the sense of threat, are used. This means that the subjective perception of threat by a person should be confronted with the knowledge, experience and psychology of reactions of the general public, objectified through the sense of threat in given circumstances that would accompany the average person[29]. A justified sense of humiliation concerns the situation involving offending the dignity, diminishing the victim's value, degradation or showing disrespect, while torment is understood as causing suffering, especially mental suffering[30]. If the harassment is not so serious as to be seen as

[24] Article 190a of the Penal Code was added under Act of 25 February 2011 amending the act – Penal Code, Journal of Laws of 2011 No. 72, item 381.
[25] The sentence of imprisonment was increased to 8 years by the amendment to the Penal Code of 31 March 2020 (under the Act of 31 March 2020 amending the act on specific solutions related to the preventing, counteracting and combating COVID-19, other infectious diseases and crisis situations caused by them, and some other acts, Polish Journal of Laws of 2020 item 568). Previously, the crime was punishable by imprisonment of up to 3 years.
[26] A. Grześkowiak, K. Wiak (eds.), *Kodeks karny. Komentarz, Art. 190a*, Wyd. 7, Warszawa 2021.
[27] Ibidem.
[28] cf. Judgement of the Court of Appeal in Wroclaw – 2nd Criminal Division as of 19 February 2014, court file no. II AKa 18/14.
[29] Judgement of the Supreme Court – Criminal Chamber as of 29 March 2017, court file no. IV KK 413/16.
[30] A. Grześkowiak, K. Wiak (eds.*), Kodeks karny. Komentarz, Art. 190a*… op. cit.

a crime under Art. 190a of the Penal Code, Art. 107 of the Petty Offence Code may apply. According to it, anyone who, in order to tease another person, maliciously misleads them or otherwise maliciously disturbs them, is subject to the penalty of restriction of liberty, a fine of up to PLN 1,500 or a reprimand. Also in this case the protected value is mental peace and a state free from distress or anxiety[31].

Cyberbullying may involve threats against women or their close ones. Pursuant to Art. 190 of the Penal Code, whoever threatens another person with a crime to their detriment or the detriment of their closest person, and if the threat raises a justified fear that it will be fulfilled, is subject to a fine, restriction of liberty or imprisonment for up to 2 years. The protected value in the case of this crime is mental freedom, sense of security corresponding to their subjective sense of threat[32]. The essence of the threat is influencing the victim's psyche by evoking a state of well-founded fear that the threatened harm may befall them. The Penal Code does not enumerate offenses involving threat. Consequently, these will be all activities that constitute a prohibited act. Women are particularly vulnerable to threats of beating, kidnapping, killing and sexual violence expressed on the Internet[33]. According to the judicial practice of the Supreme Court, "in order to meet the criteria of a crime under Art. 190 § 1 of the Penal Code, it is not required that the perpetrator actually intends to carry out the threat or that he or she undertakes any actions aimed at immediate fulfilment of their threat. It is enough to show that the threat, subjectively, i.e. in the perception of the endangered person, induced a fear of its fulfilment, and then this fact should be verified by determining objectively whether the threatened person could, in the given circumstances, perceive the threat in this manner"[34]. An unlawful threat is an offence prosecuted under private prosecution, i.e. at the motion of the aggrieved party.

Women often fall victim to vulgar, offensive comments or content posted on the Internet, sharing photos or material that is offensive to them, slander, hate speech or name-calling. Such activities may meet the criteria of various crimes defined in the Penal Code. Art. 212 of the Penal Code defines the offense of defamation: whoever slanders another person, group of people, institution, legal person or an unincorporated organizational unit, presenting defamatory statements regarding a conduct or properties that may demean it in the public opinion or expose it to the loss of trust required for a given position, profession or type of activity, is subject to a fine or a penalty of restriction of liberty. If the slander is committed by means of mass communication, the court may also order a term of imprisonment of up to one year (Art. 212 § 2 of the Penal Code). In the case of defamation the

[31] P. Daniluk (ed.), *Kodeks wykroczeń. Komentarz, Art. 107*, Wyd. 2, Warszawa 2019.
[32] A. Grześkowiak, K. Wiak (eds.), *Kodeks karny. Komentarz, Art. 190*… op. cit.
[33] Z. Warso, J. Smętek, *Cyberprzemoc*… op. cit., p. 28.
[34] Decision of the Supreme Court – Criminal Chamber as of 5 December 2017, court file no. III KK 251/17.

protected value is respect, good name of the victim or the victim's social status[35]. Defamation is understood as accusing, imputing, ascribing to the aggrieved party a specific negative behaviour or qualities in order to humiliate them in the public opinion or make them seem less trustworthy. A similar offense related to the violation of a person's personal dignity is an insult, referred to in Art. 216 of the Penal Code. The article stipulates that whoever insults another person in their presence or even in their absence, but in public or with the intention that the insult reaches that person, is subject to a fine or the penalty of restriction of liberty. If the insult was made by means of mass communication, the court may also order a term of imprisonment of up to one year (Art. 216 § 2 of the Penal Code). The main difference between defamation and insult is the object of protection. Defamation affects the so-called external dignity of a human being, their good name and perception in society. Insult, on the other hand, is an attack on internal dignity aimed at ridiculing, offending or hurting the feelings of the aggrieved party[36]. Insult must be assessed based on objective criteria; the behaviour should be generally considered offensive and violating the personal dignity of a person in the light of accepted social and moral norms[37]. When an insult is a form of cyberbullying, it is possible to classify the act as both the basic type and the qualified type (subject to a higher penalty, as defined in Art. 216 § 2 of the Penal Code). This will depend on whether the information provided is available to a large public, e.g. as a result of its publication on generally available social media or sending it to a wide group of recipients[38].

Art. 256 and 257 of the Penal Code also criminalize hate speech, i.e. public incitement to hatred or making insults for the reason of someone belonging to a given group. However, these articles only cover categories such as nationality, ethnicity, race, religion or non-religion, and do not include gender or sexuality. Publicly praising or encouraging violence against women on the Internet will fulfil the criteria presented in these articles only if such behaviour is directed against women belonging to one of the above categories, e.g. refugee women or women of a certain religion. Publishing content on the Internet that is degrading to women, offensive, contemptuous, inciting violence may be classified as public incitement to commit a crime and praising a crime under Art. 255 of the Penal Code. Pursuant to the article, all activities inciting or expressing approval for any behaviour that fulfils the criteria of a prohibited act under Polish criminal law may be penalized[39].

[35] A. Grześkowiak, K. Wiak (eds.), *Kodeks karny. Komentarz, Art. 212…* op. cit.
[36] Ibidem.
[36] Ibidem.
[37] Ibidem.
[38] Z. Warso, J. Smętek, *Cyberprzemoc…* op. cit., p. 30.
[39] A. Grześkowiak, K. Wiak (eds.), *Kodeks karny. Komentarz, Art. 255…* op. cit.

The second group of crimes contains all forms of sexual violence against women. Publishing or distributing intimate or erotic content without the consent of the person concerned, i.e. revenge pornography, is criminalized under Art. 191a of the Penal Code. Pursuant to Art. 191a § 1 of the Penal Code, whoever preserves an image of a naked person or person during sexual activity using force, unlawful threat or deception, or distributes the image of a naked person or person during sexual activity without their consent, is subject to the penalty of deprivation of liberty from 3 months to 5 years. This article was added to the Penal Code in 2009[40] due to the increasing frequency of this type of occurrences in social life and the development of technology allowing image or footage to be recorded and instantly distributed. Art. 191a of the Penal Code penalizes two types of conduct: preserving the image of a naked person or person in the course of performing sexual activity with the use of violence, threat or deception and distributing of such image without consent of that person. In the case of cyberbullying and revenge pornography, the second type will primarily apply. For the applicability of Art. 191a of the Penal Code, it does not matter whether the materials were obtained with the use of violence or coercion or with the consent of the victim – what is important is the lack of consent to their distribution[41]. Women who are victims of online blackmail, e.g. involving demands of sending erotic photos or videos under threat of harm, may report a crime of coercion under Art. 191 § 1 of the Penal Code. According to the article, whoever uses violence or unlawful threat against a person in order to force another person to perform, restrain from or endure a specific action, is subject to imprisonment for up to 3 years, however, the Polish Penal Code lacks provisions allowing for the criminalization of such behaviour as sending unwanted photos or messages of pornographic nature, making unsolicited or abusive sexual advances. Public presentation of pornographic content in a manner that imposes its reception is prohibited pursuant to Art. 202 § 1 of the Penal Code, however, this article refers only to the situation of displaying such content to the public view, so that it can reach a wider anonymous group of recipients[42].

A much broader level of protection is provided for minors. If the addressee of sexual messages or proposals is a girl under 15 years of age, Art. 200 and 200a of the Penal Code shall apply. Pursuant to Art. 200 § 3 of the Penal Code, anyone who presents pornographic content to a minor under the age of 15 or provides them with items of such nature or disseminates pornographic content in a way that allows such a minor to become acquainted with it, is subject to imprisonment for up to 3 years.

[40] Article 191a of the Penal Code was added under Act of 5 November 2009 amending the act – Penal Code, the act – Code of Criminal Procedure, the act – Executive Penal Code, the act – Fiscal Penal Code together with other acts, Journal of Laws of 2009 No. 206, item 1589.
[41] A. Grześkowiak, K. Wiak (eds.), *Kodeks karny. Komentarz, Art. 191a…* op. cit.
[42] A. Grześkowiak, K. Wiak (eds.), *Kodeks karny. Komentarz, Art. 202…* op. cit.

Art. 200a § 2 of the Penal Code stipulates, on the other hand, that whoever makes an offer of sexual intercourse, submission to or performance of other sexual activity, or participation in the production or recording of pornographic content, to a minor under the age of 15, via the ICT system or telecommunications network, and intends to implement it, shall be subject to a fine or penalty of restriction of liberty or imprisonment for up to 2 years. In the case of sexual offers, the behaviour is criminalized regardless of the minor's consent or lack thereof.

The third group of cyber violence crimes concerns identity and data theft. Pursuant to Art. 190 a § 2 a person who, by impersonating another person, uses their image, their personal data or other data by means of which this person is publicly identified, in order to inflict material or personal damage on them, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years. Impersonating someone else is understood as misleading others as to one's identity. This article covers all behaviours related to posting photos, disclosing private information, ordering various goods or services at the victim's expense, creating accounts on social networks[43]. The crime of data theft has been defined in Art. 267 § 1 of the Penal Code, according to which the person who without authorization gains access to information not intended for them by opening a closed letter, accessing the telecommunications network or breaking or bypassing electronic, magnetic, IT or other special security measures, is subject to a fine, the penalty of restriction of liberty or imprisonment for up to 2 years.

[43] R.A. Stefański (ed.), *Kodeks karny. Komentarz, Art. 190a*, Wyd. 5, Warszawa 2020.

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości"

Cyber violence in the civil law

Women who are victims of cyberbullying may make a personal right infringement claim under civil law. Art. 23 of the Civil Code includes an open catalogue of personal rights and lists, inter alia, freedom, dignity or image. Any person whose personal rights have been violated may file an action for the protection of personal rights. Pursuant to Art. 24 of the Civil Code, the aggrieved party may demand that the infringer discontinues such action, completes the actions necessary to remove its effects and submits a declaration of appropriate content and form (e.g. a written apology). Under the provisions of the Civil Code, the aggrieved party may also request financial compensation or payment of an appropriate amount of money for the indicated social purpose. The greatest difficulty in claiming rights through civil proceedings is the fact that the aggrieved party is required to provide the defendant's personal data, including their full name and address. At the same time, the perpetrators on the Internet are often unknown and anonymous, and the aggrieved women are not able to determine their personal data necessary to file a lawsuit[44]. Research conducted by the Pew Research Center shows that over 50% of perpetrators are unknown or do not reveal their true identity[45].

[44] Z. Warso, J. Smętek, *Cyberprzemoc*… op. cit., p. 32.
[45] Pew Research Center, *Online Harassment*, October 2014, p. 28, [available at:] http://www.pewinternet.org/2014/10/22/online-harassment.

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości"

Scale of cyber violence

The scale of violence against women and girls on the Internet is difficult to estimate. There has been no gender-specific research on cyberbullying in the European Union, and data from Member States is also fragmentary[46]. UN Woman, an organization dealing with gender equality and women's empowerment, reports that 73% of women worldwide have experienced at least one form of online violence[47]. Women are 27 times more likely to experience cyberbullying than men, who are perpetrators of it in 61% of the cases[48]. Pew Research Center, an American research centre, in a study on Internet violence conducted in 2014 showed that 73% of adults have experienced some form of online violence and 40% were the direct victims of it[49]. These statistics show that the problem of cyberbullying is very serious and affects a wide range of Internet users, especially young women.

In the European Union, the largest amount of data on this subject was obtained as part of a study conducted in 2014 by the European Union Agency for Fundamental Rights (usually known as Fundamental Rights Agency, FRA). This survey was based on interviews with 42,000 women from all EU Member States and focused on the various forms of violence experienced by women[50]. In the context of online violence, the focus was put on two types of it: cyberstalking and sexual harassment. According to data compiled by FRA, 5% of women in the European Union have experienced at least one form of cyberstalking after the age of 15, of which 2% have fallen victim to cyberstalking within 12 months of the survey[51]. Most frequently the victims are young women. Among young women aged 18 to 29 from all Member States (around 1.5 million women), 4% experienced cyberstalking in the 12 months prior to taking part in the survey, compared to only 0.3% of women aged 60 years or older[52].

FRA defines online harassment as receiving unsolicited, abusive emails or text messages that are sexually explicit or receiving offensive, inappropriate proposals via social networks[53]. The interviews show that 11% of women over 15 years old have fallen victim to at least one form of online

[46] European Institute for Gender Equality, *Cyber…* op. cit., p. 3.
[47] UN Broadband Commission For Digital Development Working Group On Broadband And Gender, *Cyber violence…* op. cit., p. 15.
[48] Ibidem.
[49] Pew Research Center, *Online…* op. cit.
[50] FRA European Union Agency for Fundamental Rights, *Violence against women: an EU – wide survey. Main results report,* Publications Office of the European Union, Luxembourg, 2014, [available at:] https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance-oct14_pl.pdf.
[51] FRA European Union Agency for Fundamental Rights, *Violence against women: an EU – wide survey. Main results report*, Publications Office of the European Union, Luxembourg, 2014, [available at:] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf, p. 87
[52] Ibidem.
[53] Ibidem, p. 104.

harassment, of which 5% in the 12 months preceding the survey[54]. Again, young women between the ages of 18 and 29 are most at risk. The risk of experiencing cyber-harassment is twice as high as for women between 40 and 49 years old and three times greater than for women between 50 and 59 years old[55]. Young women up to the age of 29 most often encounter inappropriate offers made via social networks (53%) and unsolicited messages of a sexual nature (34%)[56]. These indicators are related to the access to the Internet and the frequency of using the network. In countries with good Internet access, the percentage of women experiencing Internet harassment is the highest in the European Union, amounting to 18% in Denmark and Sweden, and 17% in the Netherlands and Finland[57]. The lowest rates were recorded in Romania (7%), Lithuania and Portugal (8%)[58]. Moreover, research shows that cyberbullying is connected with other forms of violence. As many as 70% of women who have been victims of cyberstalking and 77% of women who have experienced online harassment have also experienced sexual or physical violence from their partner[59].

Age and gender are the main risk factors of online violence as showed by Pew Research Center's study on cyberbullying conducted in 2014. 6 types of cyberbullying were accounted for in the study: name-calling, ridicule, unlawful threats, cyberstalking, sexual harassment and mobbing[60]. Young adults up to 29 years are the most vulnerable group, 65% of respondents at this age have experienced at least one form of cyberbullying. Women in this age group experience severe forms of violence much more often than men: 26% of respondents have been victims of cyberstalking, 25% have experienced online sexual harassment[61]. Women are also much more exposed than men to the negative emotional consequences of such violence - 38% of women described their experiences with violence as very serious, as opposed to 17% of men[62]. The study shows that the most cases of violence - as much as 66% - occurred in the social media or social media applications. This value rises up to 74% of cases in the 18-29 age group.

In the case of national statistics, most European Union Member States do not have legislation that would explicitly criminalize cyberbullying, so law enforcement bodies and judicial authorities are not in possession of complete data on this subject[63]. The provisions of the Polish Penal Code discussed

[54] Ibidem.
[55] Ibidem, p. 105.
[56] Ibidem, p. 108.
[57] Ibidem.
[58] Ibidem.
[59] Ibidem.
[60] Pew Research Center, *Online*… op. cit., p. 3.
[61] Ibidem.
[62] Ibidem, p. 7.
[63] Ibidem.

in Part Two allow for the criminalization of many behaviours that constitute a form of cyberbullying. At the same time, none of these provisions applies only to activities committed with the use of communication technology. Consequently, it is not possible to estimate the scale of such crimes based on police statistics.

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości”

Conclusion

Women around the world experience various forms of gender-based violence. Due to the progressive development of communication technologies, violence in cyberspace is becoming a more and more serious threat, on a wide scale. The conceptual scope of cyberbullying includes various types of behaviour, such as stalking, harassment, intimidation, sending unsolicited messages and proposals, sexual abuse on the Internet, sharing pornographic content without consent, data theft, identity theft, publishing private and intimate content, as well as other activities with the use of communication technology that cause harm or suffering to women. The available statistics clearly show that the group most exposed to cyberbullying, including its serious forms, such as stalking and abuse, are girls and young women up to the age of 29. The phenomenon of cyberbullying is often underestimated and treated as less serious than physical or sexual violence experienced in the real world. Meanwhile, cyberbullying has serious emotional and sometimes economic consequences for its victims. Moreover, as shown in the study of the European Union Agency for Fundamental Rights, more than 70% of women who have been victims of cyberstalking or harassment on the Internet have also experienced sexual or physical violence by their partner. These data indicate that cyberbullying is not an isolated phenomenon and may occur jointly with or lead to other forms of violence. At the same time, considering the constantly growing number of Internet and social media users in the world, the scale of potential victims is huge.

In Poland, victims of cyberbullying may seek justice in civil and criminal procedure. In civil procedure it is possible to demand discontinuation of personal rights violation and be awarded compensation. As it is required to provide full personal data of the defendant, many women are not able to use this legal remedy – the vast majority of cyberbullying perpetrators remain anonymous. A proposed solution to such situation would be introducing the so-called John Doe lawsuit postulated by the Helsinki Foundation for Human Rights[64]. This would allow claims to be made against a person of unknown identity. The defendant's personal data would be determined by the court in the course of the proceedings.

The Polish Penal Code contains provisions allowing for the criminalization of various forms of cyberbullying, including insults, defamation, publishing pornographic content without consent, harassment or threats. However, there are no regulations allowing the prosecution of perpetrators of violence involving sending offensive messages, pornographic content and images, or submitting

[64] Z. Warso, J. Smętek, *Cyberprzemoc*… op. cit., p. 35.

unwanted proposals that women often receive. The effectiveness of criminal proceedings regarding cyberbullying is low. This is due to the fact that this phenomenon is treated not seriously enough by law enforcement bodies, and not enough effort is put at the stage of preparatory proceedings[65].

Elimination of violence against women, including cyberbullying, is one of the goals of the United Nations expressed in the Declaration on the Elimination of Violence against Women[66], as well as of the Council of Europe, underlined in the Istanbul Convention. Their implementation will not be possible without the involvement of states (parties) in undertaking educational activities, social campaigns and trainings for law enforcement officers and judicial officers.

[65] Ibidem.
[66] United Nations General Assembly, *Declaration on the Elimination of Violence against Women*, A/RES/48/104, 23.02.1994, available at: https://undocs.org/en/A/RES/48/104.

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości"

Bibliography

Legal acts:

1. Civil Code of 23 April 1964, Journal of Laws of 2020 item 1740.
2. Penal Code of 6 June 1997, Journal of Laws of 2020 item 1444, as amended.
3. The Council of Europe Convention on preventing and combating violence against women and domestic violence drawn up in Istanbul on 11 May 2011, Journal of Laws of 2015 item 961.
4. United Nations General Assembly, Declaration on the Elimination of Violence against Women, A/RES/48/104, 23.02.1994, available at: https://undocs.org/en/A/RES/48/104.
5. Act of 5 November 2009 amending the act – Penal Code, the act – Code of Criminal Procedure, the act – Executive Penal Code, the act – Fiscal Penal Code together with other acts, Journal of Laws of 2009 No. 206, item 1589.
6. Act of 25 February 2011 amending the act – Penal Code, Journal of Laws of 2011 No. 72, item 381.
7. Act of 31 March 2020 amending the act on specific solutions related to the preventing, counteracting and combating COVID-19, other infectious diseases and crisis situations caused by them, and some other acts (Polish Journal of Laws of 2020 item 568).

Judicial practice:

1. Judgement of the Court of Appeal in Wroclaw – 2nd Criminal Division as of 19 February 2014, court file no. II AKa 18/14.
2. Judgment of the Supreme Court – Criminal Chamber as of 29 March 2017, court file no. IV KK 413/16.
3. Decision of the Supreme Court – Criminal Chamber as of 5 December 2017, court file no. III KK 251/17.

Publications:

1. L. Blanch, W. L. Hsu, An Introduction to Violent Crime on the Internet [in:] Cyber Misbehavior, Vol. 64, No 3, 2016.
2. P. Daniluk (ed.), Kodeks wykroczeń. Komentarz, Wyd. 2, Warszawa 2019.
3. European Institute for Gender Equality, Cyber violence against women and girls, 2017.
4. European Union Agency for Fundamental Rights, Violence against women: an EU-wide survey, Publications Office of the European Union, 2015.

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości"

5. European Union Agency for Fundamental Rights, Violence against women: an EU-wide survey, Main results report, Publications Office of the European Union, Luxembourg, 2014, [available at:] https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance-oct14_pl.pdf.
6. FRA European Union Agency for Fundamental Rights, Violence against women: an EU-wide survey. Main results report, Publications Office of the European Union, Luxembourg, 2014, [available at:] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf.
7. A. Grześkowiak, K. Wiak (eds.), Kodeks karny. Komentarz, Art. 190a, Wyd. 7, Warszawa 2021.
8. Pew Research Center, Online Harassment, October 2014, p. 28, [available at:] http://www.pewinternet.org/2014/10/22/online-harassment.
9. R.A. Stefański (ed.), Kodeks karny. Komentarz, Wyd. 5, Warszawa 2020.
10. UN Broadband Commission For Digital Development Working Group On Broadband And Gender, Cyber violence against women and girls a world-wide wake-up call, [available at:] https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?vs=4259.
11. Working to Halt Online Abuse, Comparison Statistics 2003-2013, http://www.haltabuse.org/resources/stats/Cumulative2000-2013.pdf.
12. Z. Warso, J. Smętek, Cyberprzemoc wobec kobiet. Raport, Helsinki Foundation for Human Rights, Warszawa 2017, [available at:] https://www.hfhr.pl/wp-content/uploads/2017/12/HFPC-Cyberprzemoc-wobec-kobiet-raport-www.pdf.

Websites:

1. Delante, Google Bomb, https://delante.pl/definicje/google-bomb/, [accessed on 20.12.2020].
2. Global digital population as of October 2020, Statista, https://www.statista.com/statistics/617136/digital-population-worldwide, [accessed on 20.12.2020].
3. EIGE Europa, Cyber violence against women, https://eige.europa.eu/gender-based-violence/cyber-violence-against-women, [accessed on 20.12.2020]
4. S. Morgan, Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion, https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/ [accessed on 20.12.2020].

5. Sustainable Development Goals UN, Goal 9, Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation, https://sdgs.un.org/goals/goal9, [accessed on 20.12.2020].
6. UN Women, Types of violence against women and girls, https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/types-of-violence
7. Women's Media Center, Online Abuse 101, https://www.womensmediacenter.com/speech-project/online-abuse-101/#doxing, [accessed on 20.12.2020].

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości"