Articles

Studia Iuridica Lublinensia vol. 34, 4, 2025
DOI: 10.17951/sil.2025.34.4.117-129

Magdalena Lesińska-Staszczuk
Maria Curie-Skłodowska University (Lublin), Poland
ORCID: 0000-0002-7372-8604
magdalena.lesinska-staszczuk@mail.umcs.pl

Cyberviolence against Women

Z problematyki cyberprzemocy wobec kobiet

ABSTRACT

Cyberviolence is an increasingly pressing issue in today's world. Driven by technological development and widespread access to the Internet, it has become a global phenomenon unconstrained by time or space. This form of violence, manifested through harassment, abuse, and harmful behaviour on social media, has a tangible impact on everyday life, particularly for girls and women. This article analyses the phenomenon of cyberviolence against women and the legal instruments available to address it, focusing in particular on Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, as well as relevant provisions in Polish law. It also presents the scale of cyberviolence in Poland and across Europe, based on a comparison of official data and statistics collected at national and EU levels.

Keywords: cyberviolence; violence against women; cyberviolence

CORRESPONDENCE ADDRESS: Magdalena Lesińska-Staszczuk, PhD, Assistant Professor, Maria Curie-Skłodowska University (Lublin), Faculty of Political Sciences and Journalism, Głęboka 45, 20-612 Lublin, Poland.

INTRODUCTION

With the growing reach of the Internet, the widespread use of digital communication tools, and the proliferation of social media platforms, addressing and preventing cyberviolence has become a global challenge.[1]

In 1995, less than 1% of the world population had access to the Internet; within the next 25 years, this figure would rise to 59%. According to forecasts, by 2030, 95% of people worldwide will be online – and thus potentially exposed to various forms of cyberviolence. Although cyberviolence can affect Internet users of any gender and age, it disproportionately impacts women and girls.[2]

According to a 2021 study conducted by the Economist Intelligence Unit, 85% of women have encountered online violence – either by being directly targeted, witnessing it, or knowing another woman affected by it. Among them, 38% reported having personally experienced cyberviolence.[3]

This article examines the phenomenon of cyberviolence against women and the legal instruments used to address it. In addition, it presents the scale of cyberviolence in Poland and across Europe, based on a comparison of available data from official reports and statistics compiled both nationally and throughout the EU as a whole.

RESEARCH AND RESULTS

The main method used in the article is primarily the legal dogmatic method. It has been used to analyse and assess Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence,[4] as well as relevant provisions of Polish law. The analysis is also based on desk research, drawing on data from reports by the Helsinki Foundation for Human Rights,[5] the European Union Agency for Fundamental Rights,[6] and the European Fem Institute.[7]

---

[1] European Parliament resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL)) (OJ C 251/2, 30.6.2022).

[2] K. Groszkowska, *Cyberprzemoc*, "Infos (BAS)" 2022, no. 1, pp. 1–2.

[3] N. Bochyńska, A. Filipiak, J. Klimowicz, P. Prus, *Dezinformacja jako forma przemocy wobec kobiet*, Warszawa 2024, p. 16.

[4] OJ L 2024/1385, 24.5.2024.

[5] J. Smętek, Z. Warso, *Cyberprzemoc wobec kobiet*, Warszawa 2017.

[6] European Union Agency for Fundamental Rights, *Violence against Women: An EU-Wide Survey*, Luxembg 2014.

[7] S. Spurek, *Cyberprzemoc wobec kobiet w Polsce*, Bruksela 2024.

1. Understanding the concept of cyberviolence

Cyberviolence is a specific form of stalking carried out using new technologies, such as emails, text messages, or photos and videos shared online.[8]

In legal doctrine, stalking is defined as repeated and persistent persecution, manifested through various intrusive behaviours intended to harass, distress, intimidate, or otherwise disturb the victim or a person close to them.[9]

Cyberviolence should be understood as the use of Internet-based communication (in particular social media, email, or instant messaging) that causes or may cause harm, including psychological distress or suffering. Gender-based cyberviolence against women includes, for example:

- threats of rape or other forms of sexual violence, condoning or inciting violence against women, and non-consensual pornography (so-called "revenge porn");
- sexual harassment, including unsolicited sexual advances, posts, comments, private messages, and emails of a sexual nature, intended to humiliate, ridicule, or intimidate the recipient;
- creating fake profiles on erotic websites or social media (e.g. impersonation through sexually suggestive "fan pages");
- publicly disclosing information relating to a woman's private life;
- so-called erotic memes and photomontages, deepfake pornography;[10]
- posting photographs in vulgar or degrading contexts;
- sending obscene images or sexually explicit content.[11]

---

[8] UN Broadband Commission for Digital Development Working Group on Broadband and Gender, *Cyber Violence against Women and Girls: A Worldwide Wake-Up Call*, https://networkedintelligence.com/wp-content/uploads/2019/02/Cyber_violence_Gender-report.pdf (access: 20.1.2025).

[9] R. Jankowska, *Przyczyny przestępstwa uporczywego nękania*, "Kortowski Przegląd Prawniczy" 2023, no. 3, p. 24. See also M. Mozgawa, *Prawnokarne i kryminologiczne aspekty zjawiska nękania*, Warszawa 2012, p. 8.

[10] In the context of cyberviolence, the use of artificial intelligence to generate so-called deepfake pornography has become a significant phenomenon. According to the publication *The State of Deepfakes: Landscape, Threats, and Impact*, as many as 96% of deepfakes are created for this purpose. See Cyberprofilaktyka NASK, *Deepfake, Jak sztuczna inteligencja może nas oszukiwać?*, https://cyberprofilaktyka.pl/blog/deepfake-jak-sztuczna-inteligencja-moze-nas-oszukiwac_i40.html (access: 20.5.2025). Issues related to human rights and freedoms inevitably raise questions about individual obligations, which is particularly important when determining the boundaries of AI-generated outcomes. The study of artificial intelligence should therefore be approached from the perspective of potential threats to human rights. See J. Kostrubiec, *Sztuczna inteligencja a prawa i wolności człowieka*, Warszawa 2021 (e-book); A. Niewęgłowski, *Sztuczna inteligencja w prawie własności intelektualnej*, Warszawa 2021 (e-book). For a discussion on the idea of human rights and freedoms in the context of political and legal thought, see P. Lesiński, *„Wohlstand, Bildung und Freiheit für Alle". Idea praw człowieka w poglądach Gustava Struvego jako przykład radykalnej demokratycznej niemieckiej myśli polityczno-prawnej doby Wiosny Ludów*, "Krakowskie Studia z Historii Państwa i Prawa" 2022, vol. 15(4), p. 543.

[11] J. Smętek, Z. Warso, *op. cit.*, p. 10.

2. The nature and scope of the phenomenon

According to a 2017 survey by Amnesty International, one in four women using the Internet had experienced violence. Seven years later, the figure had risen to one in three. If we also include women who have witnessed cyberviolence against others, the percentage rises to nearly 70%. Furthermore, girls and young women (under the age of 25) are significantly more likely to experience online violence. Aggressive comments and remarks are often sexist and misogynistic, which can be particularly harmful to the formation of female identity during adolescence and early adulthood.[12]

The extent to which cyberviolence against women is observed clearly decreases with age. This may be due to different patterns of Internet use across age groups (in terms of intensity, online environments, and types of activity), as well as greater sensitivity among younger users to inappropriate or harmful behaviour. Nevertheless, cyberviolence affects nearly every adult woman under the age of 30.[13]

The most frequently reported forms of online violence against women in Poland include hate speech in the form of humiliation, insults, mockery, name-calling, and verbal abuse, as observed by one in three female Internet users. Slightly fewer women – around one in four – reported seeing fake profiles of women created on social media, as well as vulgar memes or manipulated images. The goal of such content, beyond humiliation or harassment of the victim, is often to spread misleading or defamatory messages widely. Criminal acts such as death threats, threats of rape or physical assault, stalking, or incitement to violence against specific women are documented less frequently. However, these figures are still alarmingly high, with more than 5% of women having encountered at least one such form of cyberviolence.[14]

Cyberviolence observed by female Internet users targets various aspects of identity, both those dependent on and independent of the individual. More than half of the respondents reported that such attacks focus on women's physical characteristics, including weight, height, body size, or dysmorphic features (i.e. appearance-related issues in general). Slightly less frequently, women reported being targeted based on their gender, sexual orientation, or their political, environmental, or social views.[15]

Although online aggression can affect individuals regardless of gender, research shows that women are more frequently targeted than men. Between 2000 and 2013, women accounted for 70% of harassment cases documented by the American organisation Working to Halt Online Abuse. Empirical research conducted in Poland

[12] S. Spurek, *op. cit.*, p. 10 ff.
[13] *Ibidem*.
[14] *Ibidem*.
[15] *Ibidem*, p. 50.

confirms that in cases involving the recording or publication of explicit images without consent (Article 191a of the Criminal Code[16]), the victims are predominantly women. Female Internet users are also frequent victims of a particular form of online extortion known as sextortion, which involves demanding explicit images or money under threat of harm or exposure of private content, including images previously shared voluntarily. According to research by the Helsinki Foundation for Human Rights, online attacks against women frequently exhibit a sexual nature or contain sexual undertones. These relate to a woman's appearance, gender, marital status, or private life.[17]

Taking into account both the scale and nature of cyberviolence against women, it must be recognised as a form of gender-based violence. This refers to violence that affects women disproportionately more than men, or that occurs specifically because of their gender. The term "gender-based violence against women" highlights the structural nature of this phenomenon and reflects historically unequal power relations, which have resulted in male dominance and the systemic discrimination of women.[18]

This concept is also linked to the persistence of gender stereotypes concerning the role of women in society. This is confirmed by the results of the Eurobarometer survey, which found that only 35% of respondents in Poland considered it unacceptable to blame women for provoking offensive responses by sharing their opinions on social media. Fifteen percent had no opinion on the matter, and a troubling 20% agreed with the statement.[19]

Data presented in a report by the Helsinki Foundation for Human Rights indicate that cyberviolence is often more than just an isolated incident. Online attacks form part of the daily experience of female politicians active on the Internet. The intensity of these attacks tends to be proportional to the public visibility of the individual. In the case of women in politics, online violence is continuous and not clearly linked to any particular trigger. Violence against women in politics is not currently addressed by any dedicated legal act. As a result, it is understood in varying ways depending on the research or institutional perspective. Some view it as encompassing various forms of violence against women who hold or seek elected public office. Other studies regard it primarily as a barrier to women's participation – both as voters and candidates – in political life. Further analyses focus specifically on online forms of violence targeting female politicians. A comprehensive report by UN Women and

[16] Act of 6 June 1997 – Criminal Code (Journal of Laws 1997, no. 88, item 553, as amended), hereinafter: CC.

[17] J. Smętek, Z. Warso, *op. cit.*, pp. 7–9.

[18] *Ibidem*.

[19] European Commission, *Gender Stereotypes – Violence Against Women*, 2024, https://europa.eu/eurobarometer/surveys/detail/3252 (access: 14.3.2025). Fieldwork was conducted between 21 and 28 February 2024; 25,835 interviews EU-wide, including 1,021 in Poland.

the Office of the United Nations High Commissioner for Human Rights highlights that, due to the lack of systematically collected data, this phenomenon remains difficult to define and analyse.[20]

Certain actions, public statements or comments may provoke a surge of aggressive content directed at women. Such aggression may also be triggered by information disclosed by third parties, e.g., press articles relating to past events. Women are at risk of being targeted when their behaviour deviates from socially assigned gender roles. The mere pursuit a profession considered "male-dominated", working in a masculinised sector, or speaking out on issues typically discussed by men in the media may serve as a pretext for attacks. Similarly, addressing topics perceived as feminist, such as reproductive rights, may also incite cyberviolence against women.[21]

An analysis of attacks provoked by women's online activity reveals that the purpose of these acts is not to initiate any substantive debate. Most of the attackers barely engage with the actual content of the woman's statement. Instead, such statements serve merely as a pretext for cyberviolence. The content of the attacks is generally unrelated to the woman's professional or personal activity. What these assaults have in common is their sexist nature, reinforcing the argument that cyberviolence against women is indeed gender-based violence. Women who are targeted often observe that men also experience online abuse. However, they consistently emphasise that it occurs with less intensity and takes a different form.[22]

According to a study conducted by the Helsinki Foundation for Human Rights, the consequences of cyberviolence can result in a reduction of women's activity not only online, but also in everyday life. This withdrawal may occur both consciously and unconsciously. When asked directly whether cyberviolence directed at them had affected their lives offline, some respondents denied any impact, while others indicated that such aggression had negatively influenced not only their emotional well-being but also their private relationships and even jeopardised their professional plans. The findings challenge the widespread belief in a distinct separation between the virtual and the real world, offering concrete examples from participants' lives that illustrate the inevitable interconnection of these two spheres. The varied experiences of respondents show that "logging off" from cyberspace and detaching oneself from the violence encountered there is not always easy, and, in some cases, may be impossible.[23]

---

[20] See also M. Druciarek, A. Niżyńska, *…To się stało już tak przezroczyste, że o tym zapominam. Przemoc wobec kobiet na polskiej scenie politycznej*, Warszawa 2020, p. 5 ff.

[21] *Ibidem*.

[22] European Institute for Gender Equality, *Cyber Violence against Women and Girls*, Vilnius 2022, p. 7.

[23] J. Smętek, Z. Warso, *op. cit.*, p. 18.

3. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence

The establishment of a comprehensive framework for the effective prevention of and response to violence against women and domestic violence within the European Union is the subject of a long-awaited Directive (EU) 2024/1385 of the European Parliament and of the Council on combating violence against women and domestic violence.[24] This Directive contributes to the implementation of the international obligations undertaken by Member States in the area of preventing and combating violence against women and domestic violence, particularly those stemming from the United Nations Convention on the Elimination of All Forms of Discrimination against Women[25] and the ILO Convention No. 190 concerning the Elimination of Violence and Harassment in the World of Work.[26]

The Istanbul Convention served as an important point of reference for the draft of the above-mentioned directive. Ratified by the European Union on 28 June 2023, it aims to prevent and combat violence against women and gender-based discrimination.[27] The Istanbul Convention is a key international treaty for addressing violence against women and domestic violence. Adopted in 2011, it is the first legally binding regional instrument that comprehensively addresses various forms of violence against women, including psychological violence, stalking,[28] physical violence, sexual violence, and sexual harassment.[29]

With regard to cyberviolence, Directive 2024/1385 defines criminal offences and corresponding penalties for certain forms of cyberviolence where such violence is inextricably linked to the use of information and communication technologies (ICT), and where these technologies are employed to substantially amplify the harmful effects of the offence, thereby altering its nature. The use of ICT entails a risk of facilitating the rapid and widespread dissemination of certain forms of cyberviolence, accompanied by a significant risk of causing severe and long-lasting harm to the victim.

---

[24] Member States shall bring into force the laws, regulations, and administrative provisions necessary to comply with this Directive by 14 June 2027.

[25] Adopted on 18 December 1979, UNTS, vol. 1249, p. 13.

[26] Adopted on 21 June 2019, entered into force on 25 June 2021.

[27] Council of Europe Convention on preventing and combating violence against women and domestic violence, Istanbul, 11.5.2011, CETS, no. 210.

[28] The criminalisation of stalking is an obligation for the signatory states of the Istanbul Convention, unless a formal reservation has been entered in respect of that provision. See M. Kulik, *Stalking w wybranych państwach europejskich systemu kontynentalnego*, [in:] *Stalking*, ed. M. Mozgawa, Warszawa 2018, p. 133 ff.

[29] European Union Agency for Fundamental Rights, *Violence against Women…*, p. 7.

Under Article 7 of Directive 2024/1385, the following acts are classified as criminal offences:

a) repeatedly or continuously engaging in threatening conduct directed at a person, at least where such conduct involves threats to commit criminal offences, by means of ICT, where such conduct is likely to cause that person to seriously fear for their own safety or the safety of dependants;
b) engaging, together with other persons, by means of ICT, in publicly accessible threatening or insulting conduct directed at a person, where such conduct is likely to cause serious psychological harm to that person;
c) the unsolicited sending, by means of ICT, of an image, video or other similar material depicting genitals to a person, where such conduct is likely to cause serious psychological harm to that person;
d) making accessible to the public, by means of ICT, material containing the personal data of a person, without that person's consent, for the purpose of inciting other persons to cause physical or serious psychological harm to that person.

Directive 2024/1385 also provides a detailed definition of cyber incitement to violence or hatred. Under its provisions, Member States are required to ensure that intentional incitement to violence or hatred directed against a group of persons, defined by reference to gender, or against a member of such a group, through the public dissemination of material containing such incitement by means of ICT, is punishable as a criminal offence.[30]

Moreover, the following acts are also recognised as criminal offences in Article 5 (1) of Directive 2024/1385:

a) making accessible to the public, by means of ICT, images, videos or similar material depicting sexually explicit activities or a person's private parts, without that person's consent, where such conduct is likely to cause serious harm to that person;
b) producing, manipulating or altering and subsequently making accessible to the public, by means of ICT, images, videos or similar material making it appear as though a person is engaged in sexually explicit activities, without that person's consent, where such conduct is likely to cause serious harm to that person;
c) threatening to engage in the conduct referred to in point (a) or (b) in order to coerce a person to do, acquiesce to or refrain from a certain act.

It should be emphasised that the increasing intensity of Internet and social media use has, in recent years, led to a sharp rise in public incitement to violence and hatred, including on grounds of gender. The easy and rapid dissemination of hate

[30] Pursuant to Article 9 of Directive 2024/1385, inciting, aiding and abetting, as well as attempting to commit a criminal offence, are also punishable as criminal offences.

speech in the digital environment is facilitated by the so-called online disinhibition effect, perceived anonymity, and a sense of impunity. Women who are targeted by sexist hate speech online are also at risk of offline escalation of hate crimes. The language used in such incitement to hatred does not always explicitly reference the gender of the person targeted; however, the biased motivation can often be inferred from the overall content or context of the message.

4. Legal regulations in Poland

Cyberviolence is a relatively broad concept, and the applicability of specific legal measures in response to such violence depends on its form and the circumstances in which it occurs. The primary instrument enabling victims of violence to enforce their rights is the Criminal Code.[31]

Article 190a § 1 CC defines the offence of persistent stalking[32] as follows: "Anyone who, through persistent harassment of another person or a person close to them, induces in them – under circumstances that justify such a response – a sense of threat, humiliation or distress, or significantly violates their privacy, shall be subject to a penalty of imprisonment for a term of between 6 months and 8 years".

According to judicial practice, persistent conduct on the part of the perpetrator is demonstrated, on the one hand, by their mental attitude – expressed through relentless harassment, i.e. persistence despite requests and warnings from the victim or other persons to cease such behaviour, and, on the other hand, by the extended duration of such behaviour.[33] The perpetrator's actions must result in the victim developing a reasonable sense of threat or experiencing a significant violation of their privacy. It is important to emphasise that the law does not require the stalker's behaviour to involve aggression. Moreover, from a legal perspective, it is irrelevant whether the perpetrator was motivated by love, hatred, a desire to annoy the victim, malice, or a need for revenge. In the opinion of the Supreme Court, the decisive factor is the victim's subjective sense of threat, which, however, must be assessed objectively – in the same manner as when evaluating a threat.[34]

The development of technology and the Internet has had a major impact on the phenomenon of persistent harassment, enabling perpetrators to target their victims more quickly and conveniently. The tools used by perpetrators, combined with

[31] K. Groszkowska, *op. cit.*, p. 3.

[32] Stalking was introduced as a criminal offence in the Polish Criminal Code in 2011.

[33] Judgment of the Court of Appeal in Wrocław of 19 February 2014, II AKa 18/14, LEX no. 1439334.

[34] Judgment of the Supreme Court of 29 March 2017, IV KK 413/16, LEX no. 2281268.

the ubiquity of digital media, make cyberstalking feel more severe and harmful to victims than stalking in the so-called real, non-virtual world.[35]

One form of cyberstalking involves making threats of violence against the victim or their close relatives. The Polish Criminal Code criminalises such behaviour under Article 190, which provides that: "Anyone who threatens to commit an offence to the detriment of another person or that person's close relative, where the threat induces in the victim a justified fear that it will be carried out, shall be subject to a fine, a restriction of liberty, or imprisonment for up to three years". According to the judicial practice of the Supreme Court, the perpetrator does not need to have a genuine intention to carry out the threat, nor do they need to take any concrete steps towards doing so. In order to meet the criteria of Article 190 CC, it is sufficient that the threat subjectively induces fear in the victim that it will be carried out, provided that the objective circumstances would reasonably allow the victim to perceive the threat in this way.[36] The threat may concern any conduct that constitutes a prohibited act, regardless of the form in which it is expressed.

It is worth noting that online harassment can take the form of publishing offensive content, slander, defamation, or hate speech. Articles 256 and 257 CC prohibit insulting or inciting hatred, but the list of protected grounds is closed and includes national, ethnic, racial, religious, and non-religious affiliation. These provisions, however, do not cover gender or sexual orientation, which are among the main grounds for discrimination. Still, content and comments directed against specific individuals may meet the criteria for private prosecution offences, such as defamation or insult. Defamation, as defined in Article 212 CC, is the imputation of conduct or characteristics to a person or group of persons that may undermine them in the estimation of the public or expose them to loss of trust necessary to perform a given office, profession, or type of activity. Defamation committed through mass media, e.g. on the Internet, constitutes grounds for the court to impose a more severe penalty. Insult, as defined in Article 216 CC, is a related offence, but concerns the violation of a person's dignity. Its purpose is to ridicule, offend, or wound the victim's feelings.[37]

Pursuant to Article 190a § 2 CC, identity theft and theft of personal data committed with the intent to cause harm are also classified as criminal offences: "Anyone who impersonates another person and uses their image, personal data, or other data by means of which the person is publicly identifiable, thereby causing property or personal harm to them, shall be liable to the same penalty".

---

[35] R. Jankowska, *op. cit*., p. 26. See also J. Grubicka, *Zjawisko stalkingu. Możliwości prawnokarnej reakcji na zachowania stalkera*, "Zagadnienia Społeczne" 2019, no. 2, p. 89.

[36] Decision of the Supreme Court of 5 December 2017, III KK 251/17, LEX no. 2408301. See also K. Groszkowska, *op. cit.*, p. 4.

[37] *Ibidem*.

The substantive scope of this offence encompasses all actions that involve misrepresentation of one's identity, such as creating accounts on social media, publishing photos, videos, posts, and comments, disclosing private information, or ordering goods and services at the victim's expense.

Furthermore, "if the act referred to in § 1 or § 2 results in the attempted suicide of the victim, the offender shall be liable to imprisonment for a term of between 2 and 15 years" (Article 190a § 3 CC).

It should also be pointed out that offences under Article 190a §§ 1 and 2 CC are prosecuted upon the motion of the injured party. This is because these offences infringe upon the sphere of personal freedom and privacy. However, Article 190a § 3 CC provides for public prosecution ex officio, due to the higher value of the protected legal interest in this case, namely human health and life.[38]

An open-ended catalogue of personality rights is set out in Article 23 of the Civil Code[39] and includes, among others, health, freedom, dignity, and image. Article 24 of the Civil Code provides for the possibility of bringing a civil action to demand the cessation of unlawful conduct, the removal of the consequences of the infringement, as well as monetary compensation or the payment of a specified amount to a designated social cause.[40] In the event of pecuniary damage, the injured party may seek compensation in accordance with the general principles of liability. To file a civil lawsuit, the personal details of the defendant must be given. Victims of cyberviolence often lack such information and are unable to obtain it. Due to the specific nature of online violence, perpetrators may remain anonymous, which prevents victims from pursuing their claims before civil courts.[41]

DISCUSSION AND CONCLUSIONS

Cyberviolence is an increasingly prevalent problem in today's world. Driven by technological development and broad access to the Internet, it has become a global phenomenon that transcends temporal and spatial boundaries. This type of violence – manifested through harassment, sexual harassment, and abuse on social media – has tangible consequences for daily life, particularly for girls and women. Unfortunately, perpetrators frequently remain anonymous and difficult to identify, which significantly undermines victims' ability to seek justice. At the same time,

[38] J. Fronczak, *Stalking z perspektywy interdyscyplinarnej*, "Białostockie Studia Prawnicze" 2013, no. 13, p. 156. See also M. Budyn-Kulik, *Kodeks karny. Komentarz do zmian wprowadzonych ustawą z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny*, LEX/el. 2011.

[39] Act of 23 April 1964 – Civil Code (Journal of Laws 1964, no. 16, item 93, as amended).

[40] See A. Michalska-Warias, K. Nazar-Gutowska, *Prawnokarne aspekty nękania w polskim prawie karnym*, "Studia Iuridica Lublinensia" 2010, vol. 14, p. 74.

[41] K. Groszkowska, *op. cit.*, p. 4.

such acts may seriously affect victims' mental health and may escalate into other forms of violence.[42]

It is therefore essential to properly assess the impact of gender-based cyberviolence on victims and to understand the mechanisms that enable perpetrators to commit such acts – in order to ensure redress, accountability, and effective prevention.

REFERENCES

Literature

Bochyńska N., Filipiak A., Klimowicz J., Prus P., *Dezinformacja jako forma przemocy wobec kobiet*, Warszawa 2024.

Budyn-Kulik M., *Kodeks karny. Komentarz do zmian wprowadzonych ustawą z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny*, LEX/el. 2011.

Druciarek M., Niżyńska N., *...To się stało już tak przezroczyste, że o tym zapominam. Przemoc wobec kobiet na polskiej scenie politycznej*, Warszawa 2020.

Fronczak J., *Stalking z perspektywy interdyscyplinarnej*, "Białostockie Studia Prawnicze" 2013, no. 13, **DOI: https://doi.org/10.15290/bsp.2013.13.13**

Groszkowska K., *Cyberprzemoc*, "Infos (BAS)" 2022, no. 1.

Grubicka J., *Zjawisko stalkingu. Możliwości prawnokarnej reakcji na zachowania stalkera*, "Zagadnienia Społeczne" 2019, no. 2.

Jankowska R., *Przyczyny przestępstwa uporczywego nękania*, "Kortowski Przegląd Prawniczy" 2023, no. 3, **DOI: https://doi.org/10.31648/kpp.9410**

Kostrubiec J., *Sztuczna inteligencja a prawa i wolności człowieka*, Warszawa 2021 (e-book).

Kulik M., *Stalking w wybranych państwach europejskich systemu kontynentalnego*, [in:] *Stalking*, ed. M. Mozgawa, Warszawa 2018.

Lesiński P., *„Wohlstand, Bildung und Freiheit für Alle". Idea praw człowieka w poglądach Gustava Struvego jako przykład radykalnej demokratycznej niemieckiej myśli polityczno-prawnej doby Wiosny Ludów*, "Krakowskie Studia z Historii Państwa i Prawa" 2022, vol. 15(4), **DOI: https://doi.org/10.4467/20844131KS.22.038.16735**

Michalska-Warias A., Nazar-Gutowska K., *Prawnokarne aspekty nękania w polskim prawie karnym*, "Studia Iuridica Lublinensia" 2010, vol. 14.

Mozgawa M., *Prawnokarne i kryminologiczne aspekty zjawiska nękania*, Warszawa 2012.

Niewęgłowski A., *Sztuczna inteligencja w prawie własności intelektualnej*, Warszawa 2021 (e-book).

Smętek J., Warso Z., *Cyberprzemoc wobec kobiet*, Warszawa 2017.

Spurek S., *Cyberprzemoc wobec kobiet w Polsce*, Bruksela 2024.

Online sources

Cyberprofilaktyka NASK, *Deepfake, Jak sztuczna inteligencja może nas oszukiwać?*, https://cyberprofilaktyka.pl/blog/deepfake-jak-sztuczna-inteligencja-moze-nas-oszukiwac_i40.html (access: 20.5.2025).

[42] *Ibidem*.

European Commission, *Gender Stereotypes – Violence Against Women*, 2024, https://europa.eu/eurobarometer/surveys/detail/3252 (access: 14.3.2025).
UN Broadband Commission for Digital Development Working Group on Broadband and Gender, *Cyber Violence against Women and Girls: A Worldwide Wake-Up Call*, https://networkedintelligence.com/wp-content/uploads/2019/02/Cyber_violence_Gender-report.pdf (access: 20.1.2025).

Documents

European Institute for Gender Equality, *Cyber Violence against Women and Girls*, Vilnius 2022.
European Union Agency for Fundamental Rights, *Violence against Women: An EU-Wide Survey*, Luxembourg 2014.

Legal acts

Act of 23 April 1964 – Civil Code (Journal of Laws 1964, no. 16, item 93, as amended).
Act of 6 June 1997 – Criminal Code (Journal of Laws 1997, no. 88, item 553, as amended).
Convention on the Elimination of All Forms of Discrimination against Women, adopted on 18 December 1979, UNTS, vol. 1249.
Council of Europe Convention on preventing and combating violence against women and domestic violence, Istanbul, 11.5.2011, Council of Europe Treaty Series, no. 210.
Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence (OJ L 2024/1385, 24.5.2024).
European Parliament resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL)) (OJ C 251/2, 30.6.2022).
ILO Convention No. 190 concerning the Elimination of Violence and Harassment in the World of Work and Recommendation No. 206, adopted on 21 June 2019, entered into force on 25 June 2021.

Case law

Decision of the Supreme Court of 5 December 2017, III KK 251/17, LEX no. 2408301.
Judgment of the Court of Appeal in Wrocław of 19 February 2014, II AKa 18/14, LEX no. 1439334.
Judgment of the Supreme Court of 29 March 2017, IV KK 413/16, LEX no. 2281268.

ABSTRAKT

Cyberprzemoc stanowi narastający problem we współczesnym świecie. Ze względu na rozwój technologiczny i dostęp do Internetu cyberprzemoc stała się zjawiskiem globalnym, nieograniczonym czasem i przestrzenią. Przemoc ta, pod postacią nękania, molestowania i nadużyć w mediach społecznościowych, niesie za sobą skutki dla życia codziennego, szczególnie dziewcząt i kobiet. Przedmiotem artykułu jest analiza zjawiska cyberprzemocy wobec kobiet, rozwiązań prawnych do walki z tym procederem na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2024/1385 z dnia 14 maja 2024 r. w sprawie zwalczania przemocy wobec kobiet i przemocy domowej oraz uregulowań prawnych dostępnych w prawie polskim. Ponadto przedstawiono skalę występowania cyberprzemocy w Polsce i Europie poprzez porównanie dostępnych danych z oficjalnych raportów i statystyk tworzonych na poziomie Polski i Unii Europejskiej.

Słowa kluczowe: cyberprzemoc; przemoc wobec kobiet; cybernękanie