

Сорока Л.В.,
доктор юридичних наук, професор,
завідувачка відділу докторантури і аспірантури
Науково-дослідний інститут публічного права

ГЕНДЕРНИЙ АСПЕКТ ПРОТИДІЇ ЦИФРОВОМУ НАСИЛЬСТВУ

GENDER ASPECT OF COMBATING DIGITAL VIOLENCE

У статті аналізуються різні зарубіжні та вітчизняні нормативно-правові акти щодо протидії цифровому насильству. Визначено, що цифрова революція має як позитивні, так і негативні наслідки у гендерній сфері. Незважаючи на стрімкий ріст цифрового насильства технологічні компанії та політики продовжують надавати більше значення та захисту авторського права, ніж людей і наших прав в Інтернеті. Констатовано, що цифрове насильство охоплює широкий спектр різноманітних протиправних дій в Інтернеті. Визначено чотири основні типи насильства в Інтернеті та за допомогою технологій: 1) переслідування і насильство, здійснені за допомогою технологій (наприклад, шпигунське програмне забезпечення та інші пристрої відстеження); 2) насильство в цифровому форматі (наприклад, обмін інтимними зображеннями без згоди); 3) фейкова порнографія та зловживання цифровими особистостями (наприклад, аватари та дипфейки) та 4) використання онлайн-середовища для насильства (наприклад, сексуальне насильство через соціальні медіа). Які мають спільні риси: вони вчиняються в цифровому просторі та/або за допомогою цифрових засобів зв'язку, таких як електронна пошта чи текстові повідомлення та їх метою є – контроль. Проаналізовано Стамбульська конвенція та Загальна рекомендація GREVIO №1 щодо цифрового виміру насильства стосовно жінок, які рекомендують розробляти конкретні дії, що будуть включати профілактику, захист, судове переслідування та скоординовану політику. Визначено, що попри відсутність у вітчизняному законодавстві відповідальності за вчинення цифрового насильства, необхідно підходити до вирішення зазначеної проблеми комплексно: розробити стандартизовані визначення, методології, показники та принципи моніторингу; інвестувати в якісні дослідження, які є ключовими для виявлення нових форм цифрового насильства; навчати навичкам виявлення та фіксації цифрового насильства і створити національну правову базу на підставі міжнародних принципів і стандартів.

Ключові слова: гендер, гендерна політика, цифрове насильство, моніторинг, законодавча база, міжнародні стандарти, протидія, захист.

The article analyzes various foreign and domestic legal acts on countering digital violence. It was determined that the digital revolution has both positive and negative consequences in the gender sphere. Despite the rapid rise of digital violence, technology companies and politicians continue to place more importance and protection on copyright than people and our rights on the Internet. It has been established that digital violence covers a wide range of different illegal activities on the Internet. Four main types of online and technology-based violence have been identified: 1) technology-based harassment and violence (eg, spyware and other tracking devices); 2) digital violence (for example, sharing intimate images without consent); 3) fake pornography and abuse of digital identities (e.g. avatars and deepfakes) and 4) use of the online environment for violence (e.g. sexual assault via social media). What they have in common: they are committed in the digital space and/or through digital means of communication such as e-mail or text messages and their purpose is to control. The Istanbul Convention and GREVIO General Recommendation No. 1 on the digital dimension of violence against women are analyzed, recommending the development of concrete actions that will include prevention, protection, prosecution and coordinated policies. It was determined that despite the absence of responsibility for the commission of digital violence in domestic legislation, it is necessary to approach the solution of the specified problem comprehensively: develop standardized definitions, methodologies, indicators and principles of monitoring; invest in quality research that is key to identifying new forms of digital violence; teach skills to detect and record digital violence and create a national legal framework based on international principles and standards.

Key words: gender, gender policy, digital violence, monitoring, legal framework, international standards, counteraction, protection.

Вступ. Цифрова революція та впровадження онлайн-інформаційних і комунікаційних технологій мають як позитивні, так і негативні гендерні наслідки. З одного боку, онлайн-простори та цифрові інструменти можуть полегшити доступ до важливої інформації та послуг, розкриваючи можливості для отримання освіти та працевлаштування для жінок і дівчат. Але з іншого боку, зростає кількість доказів, які проливають світло на те, як цифрова революція загострила існуючі та навіть створила нові форми гендерної нерівності, гноблення та сприяє насильству над жінками і дівчатами [1, с. 175].

Останніми роками, особливо на тлі тривалої пандемії [2; 3], яка ще більше змінила життя людей в Інтернеті, цифрове насильство, привернуло увагу науковців, захисників цифрових прав, рухів за права, постачальників цифрових послуг та інших, хто хоче зрозуміти та оцінити його масштаб. За даними Economist Intelligence Unit, 85% жінок повідомили, що були свідками насильства в Інтернеті, а майже 40% пережили це особисто. Жінки та дівчата, меншини та маргіналізовані верстви населення найімовірніше зазнають зловживання в Інтернеті [4]. Ця зростаюча хвиля женоненависті та насильства є руйнівною для тих, хто її відчуває. Проте це ігнорується технологічними компаніями та політиками, які продовжують надавати більше значення та захисту авторського права, ніж людей і наших прав в Інтернеті.

Цифрове насильство як відносно нове явище, досліджувалося різними фахівцями. Існує невелика, але зростаюча колекція робіт на цю тему, включаючи кілька емпіричних досліджень. Так, наприклад, гуманітарна організація Plan International [5] регулярно публікує звіти про стан дівчат у світі. Останній її звіт під назвою «Стан дівчат у світі 2021: розрив правди» (State of the World's Girls 2021: The Truth Gap) [6], присвячений темі як дівчата-підлітки та молоді жінки справляються з дезінформацією під час спілкування з політичними, громадянськими чи соціальними темами в Інтернеті. Інший авторський проєкт: «Сексуальне насильство на основі зображень. Дослідження причин і наслідків оголених або сексуальних зображень без згоди» (Image-based Sexual Abuse. A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery), авторами якого є: Нікола Генрі, Клер МакГлінн, Ашер Флінн, Келлі Джонсон, Анастасія Пауелл, Адріан Дж. Скотт, був присвячений аналізу причин та наслідків сексуального насильства на основі зображень у цифрову еру. Так, автори спіраючись на новаторські емпіричні дослідження, включаючи опитування в трьох країнах із понад 6000 респондентами та понад 100 інтерв'ю з постраждалими та зацікавленими сторонами, керуючись теоретичними основами гендерних досліджень, соціології, кримінології, права та психології, стверджують, що сексуальне насильство на основі зобра-

жень частіше вчиняється чоловіками, ніж жінками, і що вчинення є вищим серед деяких груп, включаючи молодих чоловіків та чоловіків із сексуальних меншин. Хоча мотивація злочинців різна, домінуючою темою стала влада та контроль. Гендерний характер насильства означає, що його найкраще розуміти як «безперервне сексуальне насильство», оскільки жертви часто переживають його як частину ширшої моделі гендерних домагань, насильства та жорстокого поводження [7].

Водночас питання протидії цифровому насильству досліджували невелика кількість вітчизняних вчених. Цікавою роботою, на нашу думку, є «Полісемія простору і цифрове насильство». У ній Сергій Вікторович Григорішин та Катерина Володимирівна Новокрещенних здійснили порівняльний аналіз соціального та цифрового простору, продемонстрував трансформацію поняття «насильство». Автори дійшли висновку, що соціальне насильство в соціальному просторі виникло в роздумах ситуаціоністів з приводу урбанізації, а цифрове насильство в цифровому середовищі є не насильством як таким, а відмовою від низки розумових операцій, фундаментальних для феноменологічного пізнання. У статті аргументовано положення про необхідність збереження поняття інтенційності для всебічного уявлення про зв'язок цифрового простору і свідомості людини [8].

Отже, метою цього дослідження є аналіз правових засад протидії цифровому насильству та виокремлення основних ознак такого насильства, що впливають на становище жінок у соціумі.

Виклад основного матеріалу. Цифрове насильство охоплює широкий спектр різноманітних протиправних дій в Інтернеті. Є одна спільна риса цих правопорушень: вони вчиняються в цифровому просторі та/або за допомогою цифрових засобів зв'язку, таких як електронна пошта чи текстові повідомлення. Смартфони та комп'ютери стали невід'ємною частиною нашого життя. Цифровізація змінила та пришвидшила багато сфер повсякденності та продовжуватиме робити це завдяки великим технічним крокам. Попри те, що багато з цих позитивних аспектів Інтернету існують, вони також мають свої негативні сторони. Нинішні події у світі, війни та дедалі більша жорстокість суспільства – це лише кілька прикладів. Інтернет стає великою платформою для шахрайства, насильства та ненависті.

Необхідно зазначити, що дискусія в першу чергу триває щодо легального визначення «цифрове насильство». В міжнародних документах воно визначається наступним чином: акт насильства, вчинений однією або декількома особами проти особи та її статі, що ґрунтується на гендерній нерівності та порушує гендерні норми і який вчиняється, сприяє та посилюється частково або повністю за допомогою інформаційних та комунікаційних технологій чи цифрових медіа [9].

Цифрове насильство може бути вчинене у різний спосіб, але основним його елементом виступає мета такого насильства – контроль жертви. Так, погрози та переслідування – це тактика, яка зазвичай використовується у насильстві за допомогою технологій. Зловмисники вдаються до залякування, бомбардуючи жертв шквалом дзвінків, текстових повідомлень, електронних листів та інших цифрових повідомлень. Вони також можуть вдаватися до публікації принизливого вмісту в Інтернеті з наміром очорнити чиюсь репутацію. Зловмисники маніпулюють налаштуваннями та обліковими записами і таким чином впливають на життя людини, а також на її зв'язок із друзями, родиною та колегами. Більше того, деякі зловмисники доходять до того, що змушують когось відповідати на їхні дзвінки та повідомлення проти їхньої волі, фактично підриваючи автономію та свободу жертви.

З вищесказаного випливають чотири основні типи або категорії насильства в Інтернеті та за допомогою технологій:

– по-перше, це різні форми переслідувань, насильства чи жорстокого поводження, яким сприяють певні технології та технологічні пристрої (наприклад, насильство з боку інтимного партнера, яке здійснюється за допомогою технологій, включаючи шпигунське програмне забезпечення та інші пристрої відстеження);

– по-друге, насильство, яке відбувається та посилюється в цифровому форматі (наприклад, різні форми сексуального насильства на основі зображень, як-от обмін інтимними зображеннями без згоди);

– по-третє, фейкова порнографія та зловживання нашим цифровим «я» в метавесвіті (наприклад, аватари та дипфейки);

– по-четверте, коли онлайн-середовище використовується для насильства та жорстокого поводження (наприклад, використання соціальних медіа є центральним у різних формах сексуального насильства щодо жінок і дівчат) [1].

З огляду на актуальність протидії цифровому насильству в Україні постає питання – чи існує юридичний механізм притягнення винних до відповідальності?

Основними нормативно-правовими актами, які спрямовані на забезпечення належного стану інформаційної безпеки в сучасній Україні зокрема є закони України: «Про інформацію», «Про доступ до публічної інформації», «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України»; указ Президента України від 08.07.2009 року № 514/2009 «Про доктрину інформаційної безпеки України» та деякі інші нормативно-правові акти [10]. Наприклад, Законом України «Про основні засади забезпечення кібербезпеки України» визначено поняття «кіберзлочин» (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочинним міжнародними договорами України [11]. Однак, норм які б встановлювали відповідальність за цифрове насильство, на жаль, в національному законодавстві немає.

Україна, ратифікувавши у 2022 році Стамбульську конвенцію, взяла на себе ряд зобов'язань, в тому числі виконувати рекомендації, які надає GREVIO (орган незалежних експертів, який відповідає за моніторинг виконання сторонами Конвенції Ради Європи про запобігання та боротьбу з насильством щодо жінок і домашнім насильством) [12]. Він ще у 2021 році прийняв першу Загальну рекомендацію №1 щодо цифрового виміру насильства стосовно жінок. У ній визначено конкретні дії, засновані на чотирьох стовпах Стамбульської конвенції: профілактика, захист, судове переслідування та скоординована політика. І хоча рекомендації GREVIO не є юридично обов'язковими, вони служать важливим орієнтиром для України, адже містять чіткі вказівки, які можуть сприяти ефективній реалізації положень Стамбульської конвенції, а саме: 1) прийняття країнами-членами спеціального законодавства щодо різних форм онлайн-насильства та цифрового насильства, таких як кіберпереслідування, доксінг, невірний обмін інтимними зображеннями та кіберпереслідування; 2) проведення кампаній з підвищення обізнаності громадськості щодо форм, наслідків та неприйнятності цифрового насильства щодо жінок та запровадження освітніх програм в школах щодо поведінки в Інтернеті та безпеці цифрового насильства; 3) розроблення та фінансування спеціалізованих служб підтримки для жертв цифрового насильства, зокрема телефони довіри, консультації та юридична допомога; 4) навчання правоохоронних, судових органів і постачальників послуг підтримки з метою вчасного розпізнавання випадків цифрового насильства та розглядати їх; 5) покращення збору даних про випадки цифрового

насильства щодо жінок, щоб краще зрозуміти масштаб і природу проблеми; 6) підтримання проведення досліджень причин, наслідків та ефективних заходів реагування на цифрове насильство; 7) заохочення співпраці між урядами та технологічними компаніями для розробки інструментів і політики для запобігання та реагування на цифрове насильство; 8) співпраця з платформами соціальних мереж та іншими онлайн-сервісами, щоб створити чіткі та доступні механізми звітності для користувачів, які зазнають цифрового насильства; 9) посилення заходів щодо протидії цифровому насильству та притягнення винних до відповідальності, в тому числі шляхом міжнародної співпраці у випадках, коли правопорушники знаходяться в різних юрисдикціях.

Ці рекомендації спрямовані на створення безпечнішого цифрового середовища для жінок і забезпечення ефективного вирішення та запобігання насильству щодо жінок у будь-якій формі.

Таким чином, цифрове насильство проти жінок включає широкий спектр протиправної поведінки. Технології розвиваються дуже швидко, і малоімовірно, що будь-які правові норми чи етичні кодекси встигнуть за ними. З іншого боку, площина ризику надто багатовимірна: дипфейки використовуються для порно помсти, крадіжки даних або навіть крадіжки особистих даних. Фейкові відео поширюються в чутливі періоди: перед виборами, під час заворушень чи соціальних криз. Як наслідок, багато прав порушуються, а межа між правдою

та брехнею стирається. Дехто навіть запропонував створити Декларацію прав на аватар, тож чи стане це питанням часу, коли штучний інтелект стане рівним статусу людей [13; 14]?

Висновки. Сьогодні більшість піднятих питань не мають однозначної відповіді – ні серед розробників, ні серед науковців. І вихід точно не в постановах чи заявах правозахисників. Принаймні, не найближчим часом. Однак це не означає, що ми повинні мовчати про проблему або перестати шукати відповіді на поставленні питання. Ми все ще можемо відрізнити реальне від синтезованого, але технології вдосконалюються з кожним днем. І краще малювати чіткі «червоні лінії» до того, як лінія повністю стерлася [13]. Отже, попри вигоди та інноваційний потенціал цифрового світу, жінки та дівчатка з усього світу все більше висловлюються з приводу шкідливого, сексистського, женонависницького та насильницького контенту та поведінки у цифровому просторі [15]. І тому важливо визнати, що для подолання цифрового насильства щодо жінок і дівчат недостатньо створити заборони і обмеження. Необхідно підходити до вирішення зазначеної проблеми комплексно: розробити стандартизовані визначення, методології, показники та принципи моніторингу; інвестувати в якісні дослідження, які є ключовими для виявлення нових форм цифрового насильства; навчати навичкам виявлення та фіксації цифрового насильства і створити національну правову базу на підставі міжнародних принципів і стандартів.

СПИСОК ЛІТЕРАТУРИ:

1. Сорока Л. В. Цифрове насильство щодо жінок і дівчат. Гендерна політика в умовах воєнного стану: правовий вимір : збірник тез доповідей міжнародної науково-практичної конференції 15 червня 2023 р. Науково-дослідний інститут публічного права. Одеса : Видавництво «Юридика», 2023. С. 175-178.
2. Flor LS, Friedman J, Spencer CN, et al. Quantifying the effects of the COVID-19 pandemic on gender equality on health, social, and economic indicators: a comprehensive review of data from March, 2020, to September, 2021. *The Lancet* 2022; 399:2381–97. URL: <https://pubmed.ncbi.nlm.nih.gov/35247311/>
3. Bhatia A, Fabbri C, Cerna-Turoff I, et al. Violence against children during the COVID-19 pandemic. *Bull World Health Organ* 2021;99:730–8. URL: <https://pubmed.ncbi.nlm.nih.gov/34621091/>
4. Digital Violence is Violence. UNFPA, 2024. URL: <https://www.unfpa.org/digital-violence-violence>
5. The organisation. Plan International, 2024. URL: <https://plan-international.org/organisation/>
6. State of the World's Girls 2021: The Truth Gap. Plan International, 2024. URL: <https://plan-international.org/publications/the-truth-gap/>
7. Henry, Nicola, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, Adrian J. Scott. *Image-based Sexual Abuse A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery*. Routledge, 2020. URL: <https://www.routledge.com/Image-based-Sexual-Abuse-A-Study-on-the-Causes-and-Consequences-of-Non-consensual-Nude-or-Sexual-Imagery/Henry-McGlynn-Flynn-Johnson-Powell-Scott/p/book/9780367524401>
8. Григоришин С. В., Новокрещенних К. В. Полісемія простору і цифрове насилля. *Epistemological Studies in Philosophy, Social and Political Sciences*, 2021, 4 (1). С. 38–50.
9. Reporting Tip sheet on Digital Violence: A practical reference guide for journalists and media. UNFPA, 2021. URL: <https://www.unfpa.org/resources/digital-violence-tip-sheet-for-journalists>
10. Кіндрись М. Рекомендації щодо удосконалення національного законодавства України щодо захисту прав осіб, постраждалих від насильства в цифровому середовищі. Аналітичний центр ЮрФем, 2023. URL: <https://jurfem.com.ua/recomendatsii-schodo-udoskonalennya-zakonodavstva-zyfr-seredovysche/>
11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Верховна Рада України* офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
12. About GREVIO – Group of Experts on Action against Violence against Women and Domestic Violence. Council of Europe Portal, 2024. URL: <https://www.coe.int/en/web/istanbul-convention/grevio>
13. Avdieieva T. Who is hiding behind digital avatars? Centre for Democracy and Rule of Law, 2021. URL: <https://cedem.org.ua/en/analytics/tsyfrovii-avatory/>
14. Soroka, Larysa (2023) Modern Views on Criminal Liability for Crimes in Outer Space. *Philosophy and Cosmology*, Volume 30, 64–76. <https://doi.org/10.29202/phil-cosm/30/6>
15. Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective. A/HRC/38/47 UN. Human Rights Council, 2018. URL: <https://digitallibrary.un.org/record/1641160>