

Серебро М. В.,

*кандидат юридичних наук, доцент, докторант
Державного вищого навчального закладу
"Ужгородський національний університет"
м. Ужгород, Україна*

НАПРЯМИ УДОСКОНАЛЕННЯ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

Правовою основою протидії правопорушенням у сфері використання інформаційних технологій є відповідні положення Кодексу України про адміністративні правопорушення та Кримінального кодексу України.

Так, окремий Розділ XVI КК України присвячений кримінальним правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Зокрема, ст. 361 КК України передбачено відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [1].

Статтею 361-1 КК України передбачено відповідальність за створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут [1].

Крім того, ст. 361-2 КК України передбачено відповідальність за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації [1].

Відповідальність за несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, передбачена ст. 362 КК України [1].

Статтею 363 КК України передбачена відповідальність за порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється.

Крім того, ст. 363-1 КК України встановлено відповідальність за перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [1].

Таким чином, ст. 363-1 КК України передбачає кримінальну відповідальність за поширення спаму, якщо вказані дії призвели до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Проте актуальним залишається питання встановлення адміністративної відповідальності за систематичне поширення спаму без настання вказаних наслідків.

Таким чином, актуальним вбачається встановлення адміністративної відповідальності за поширення спаму, тобто умисне систематичне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що не призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Крім того, народні депутати хочуть ввести до законодавства України поняття stalking – переслідування особи. Йдеться не лише про фізичне стеження, а й переслідування особи через соціальні мережі. Про це йдеться у пояснювальній записці до законопроекту №12088 про внесення змін до Кримінального процесуального кодексу та закону «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за злочинне переслідування (stalking) [2].

Вперше поняття «stalking» з'явилося на законодавчому рівні як правопорушення, за яке передбачена кримінальна відповідальність, наприкінці двадцятого століття у США (штат Каліфорнія). Відповідно до положень Кримінального кодексу штату, «stalking» визначено як свідоме, здійснюване із злим умислом переслідування та спричинення занепокоєння іншій людині [3].

На розвиток положень щодо відповідальності за stalking Європейською Комісією ухвалено Директиву щодо протидії насильству над жінками та домашньому насильству №2022/0066. Нею пропонується криміналізувати кіберпереслідування (cyber stalking) як сучасну форму психологічного насильства, що часто вчиняється проти членів сім'ї або осіб, які живуть в одному будинку (може здійснюватися колишніми партнерами або знайомими) [3].

Українські парламентарі пропонують визначити кіберпереслідування як вид злочинного переслідування. Воно передбачає постійне спостереження за постраждалою особою без її згоди чи законного дозволу за допомогою інформаційних і комунікаційних технологій. Таке переслідування може здійснюватися шляхом опрацювання персо-

нальних даних жертви (в результаті крадіжки даних або шпигування за жертвою через її соцмережі чи платформи обміну повідомленнями, електронну пошту й телефон). Йдеться також про злом пристроїв особи для доступу до приватного простору за допомогою встановлення додатків геолокації, зокрема шпигунського програмного забезпечення, або через викрадення пристроїв [2].

Важливо, на думку М. Лісничук, що ці терміни автори законопроекту пропонують встановити лише в законі про домашнє насильство. До Кримінального процесуального кодексу ініціатори пропонують запровадити норму про те, що рішення суду першої інстанції про застосування обмежувального заходу до осіб, які вчинили домашнє насильство, набирає законної сили з моменту проголошення, а оскарження не зупиняє його виконання [2].

Не менш важливим є встановлення відповідальності за кібербулінг. Так, О. Коваль зазначає, що найбільш повну характеристику цьому явищу надав UNICEF, який визначає його як цькування з застосуванням цифрових технологій. Воно може відбуватися в соціальних мережах, на платформах обміну повідомленнями (месенджерах), ігрових платформах та мобільних телефонах. Це поведінка, спрямована на залякування, провокування гніву чи приниження тих, проти кого вона спрямована. Серед прикладів такого цькування можна згадати поширення брехні або розміщення фотографій, які компрометують когось, у соціальних мережах; надсилання повідомлень або погроз, які ображають когось або можуть завдати комусь шкоди, через платформи обміну повідомленнями; видання себе за когось іншого/іншу і надсилання повідомлень іншим людям від його/її імені [4].

Правові механізми захисту існують та еволюціонують. Зокрема, залежно від тяжкості наслідків, відповідальність за кібербулінг може бути як адміністративною, так і кримінальною. Більше того, вже на сьогодні включені до законодавства норми, що регулюють правопорушення, пов'язані саме з кібербулінгом. Так, адміністративна відповідальність передбачена ст. 173-4 Кодексу України про адміністративні правопорушення «Булінг (цькування) учасників освітнього процесу» [4; 5].

Українське законодавство визначає булінг (цькування) як діяння учасників освітнього процесу, які полягають у психологічному, фізичному, економічному, сексуальному насильстві, у т.ч. з застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи або такою особою стосовно інших учасників освітнього процесу, внаслідок чого могла бути чи була заподіяна шкода психічному або фізичному здоров'ю потерпілого [4; 5].

Проте, як зазначає О. Коваль, «наявність норм законодавства зовсім не гарантує реальний захист потерпілих у результаті цькування у соцмережах та понесення адекватного покарання винними за такі

діяння. Вивчаючи практику, яка відображена в Єдиному державному реєстрі судових рішень, можна зустріти поодинокі випадки, коли батьків дітей, які вчиняють цькування у мережі, притягують до адміністративної відповідальності за ч. 3 ст. 173-4 КУпАП (булінг (цькування) учасників освітнього процесу) з покладенням обов'язку сплатити штраф. Також трапляються випадки складання протоколів про притягнення до адміністративної відповідності за ст. 184 КУпАП у зв'язку з тим, що батьки не вживають заходів виховного характеру щодо своїх дітей, які систематично вчиняють кібербулінг. Але найчастіше батьки «булерів» отримують лише усні попередження» [4].

До прикладу – у постанові від 6 квітня 2021 року у справі № 647/879/21 Бериславський районний суд Херсонської області звільнив матір хлопця, який систематично вчиняв кібербулінг, від адміністративної відповідальності, обмежившись лише усним попередженням. Найбільш жорстке реальне покарання за цькування дитини в інтернеті, яке вдалося знайти О. Коваль, – це штраф у 1700 грн. Так, у справі №190/854/21 П'ятихатський районний суд Дніпропетровської області визнав винною матір (чи опікунку) дітей, які займалися інтернет-цькуванням іншої дитини, та стягнув з неї 1700 грн штрафу та 454 грн судового збору [4].

Наведені приклади свідчать про формальний та поверховий підхід до проблеми кібербулінгу в процесі правозастосування.

Для ефективної протидії кібербулінгу О. Коваль слушно пропонує створення належних умов для подання скарг та термінового звернення дітей до правозахисних інституцій – уповноваженого Верховної Ради України з прав людини, уповноваженого Президента України з прав дитини, освітнього омбудсмена [4].

Для реалізації вказаної пропозиції доцільно на рівні спільного наказу Міністерства освіти і науки України та Міністерства цифрової трансформації України регламентувати розробку мобільного додатку для учнів, в якому буде передбачена можливість прямого, безпосереднього листування із вищезазначеними суб'єктами владних повноважень. Крім того, доцільно суттєво посилювати адміністративну відповідальність за булінг (цькування) учасника освітнього процесу, яка передбачена ст. 173-4 КУпАП.

Список використаних джерел:

1. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. Дата оновлення: 19.05.2024. URL: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20240519#Text> (дата звернення: 01.10.2024).

2. Лісничук М. В Україні пропонують ввести покарання за сталкінг та переслідування в соцмережах: що відомо. 13.10.2024. Obozrevatel.com. URL: <https://news.obozrevatel.com/ukr/society/v-ukraini->

proponuyut-vvesti-pokarannya-za-stalking-ta-peresliduvannya-v-sotsmerezhhah-scho-vidomo.htm (дата звернення: 15.10.2024).

3. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Закону України «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за злочинне переслідування (сталкінг). Картка законопроекту. Пояснювальна записка. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/44972> (дата звернення: 05.10.2024).

4. Коваль О. Кібербулінг: як захистити дитину від цькування в мережі. *Юридична газета Online*. 28.09.2024. №18 (748). URL: <https://jur-gazeta.com/publications/practice/inshe/kiberbuling-yak-zahistiti-ditinu-vid-ckuvannya-v-merezhi.html> (дата звернення: 05.10.2024).

5. Кодекс України про адміністративні правопорушення. Дата оновлення: 09.08.2024. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (дата звернення: 05.10.2024).

DOI <https://doi.org/10.36059/978-966-397-502-3-43>

Томин С. В.,

*кандидат юридичних наук, доцент,
завідувач кафедри кримінального права та кримінології
Івано-Франківський навчально-науковий юридичний інститут
Національного університету «Одеська юридична академія»
м. Івано-Франківськ, Україна*

ТИПОВІ СПОСОБИ УХИЛЕННЯ ВІД ПРИЗОВУ НА ВІЙСЬКОВУ СЛУЖБУ ЯК ЕЛЕМЕНТ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО СТ. 336 КК УКРАЇНИ

У юридичній літературі виділяють три форми ухилення від призову на військову службу під час мобілізації:

- 1) неявка за повісткою у вказаний строк без поважної причини;
- 2) отримання шляхом обману незаконного звільнення від призову на військову службу;
- 3) отримання шляхом обману відстрочки від призову [1, с. 289].

Я. Ф. Фокін поділяє способи вчинення цього виду кримінальних правопорушень на дві основні групи: активні та пасивні. До активних автор відносить симуляцію хвороби або умисне спричинення собі тілесних ушкоджень, введення в оману щодо віросповідання та переконань, що дають підставу для проходження альтернативної