



АНАЛІЗ ПРАВОВОГО ПОЛЯ УКРАЇНИ ЩОДО ГЕНДЕРНО-ЗУМОВЛЕНИХ КІБЕРЗЛОЧИНІВ

Грудень 2024

Дослідження судових рішень **01.01.2023 - 30.06.2024**

АВТОРКИ:

ОКСАНА ГУЗЬ

адвокатка, експертка з питань
недискримінації, злочинів на ґрунті
ненависті та гендерної зумовленого
насильства

ГАННА ЛИТВИНОВА

юристка, експертка з безпеки, протидії
гендерно зумовленому насильству,
правозахисниця



**ГРОМАДСЬКА ОРГАНІЗАЦІЯ "ІНСАЙТ" ЗА
ПІДТРИМКИ ДАНСЬКОГО ЦЕНТРУ ДОСЛІДЖЕНЬ
ЖІНОК ТА ҐЕНДЕРУ (KVINFO)**



ЗМІСТ

Використані аббревіатури	4
Вступ	5
Розділ 1: Визначення “кіберзлочину” в українському законодавстві	7
Розділ 2: Міжнародні визначення кіберзлочинів та кібернасильства та їх розуміння в Україні	13
Розділ 3: Практики застосування в Україні	23
Розділ 4: Практика Європейського суду з прав людини	31
Розділ 5: Процедура внесення відомостей до ЄРДР	35
Розділ 6: Деякі питання доказів та доказування	39
Розділ 7: Повноваження кіберполіції	43
Розділ 8: Дослідження судових рішень	47
Розділ 9: Розвиток міжнародного законодавства	50
Висновки	52
Рекомендації	53

ВИКОРИСТАНІ АБРЕВІАТУРИ

ГЗК - гендерно зумовлені кіберзлочини

ГЗН - гендерно зумовлене насильство

ЄДРСР - Єдиний державний реєстр судових рішень

ЄРДР - Єдиний реєстр досудових розслідувань

ЄСПЛ - Європейський суд з прав людини

КК України - Кримінальний кодекс України

КПК України - Кримінальний процесуальний кодекс України

КУпАП - Кодекс України про адміністративні правопорушення

ЛГБТКІ+ - лесбійки, геї, бісексуальні, трансгендерні, квір-, інтерсекс-люди та інші

ВСТУП

У сучасному світі гендерно зумовлене насильство (далі - ГЗН), на жаль, розширює свої кордони. З тим, як швидко розвивається суспільство, цифрові технології, доступність до Інтернету та певна анонімність у цифровому світі, посуваються й межі простору для скоєння ГЗН з реального життя (офлайн) до онлайн-середовища (кіберпростір), наприклад, у соціальних мережах, месенджерах, на вебсайтах та інших інтернет-ресурсах, які ми щодня використовуємо для спілкування, навчання та роботи.

Разом із можливостями, які надає нам цифровий світ, зростає й кількість та різноманітність кіберзлочинів, зокрема тих, що мають гендерно зумовлений характер. Проте швидкість виникнення нових видів злочинів у цифровому світі перевищує швидкість законодавчого реагування державою. ГЗН іноді виникає через дискримінаційні стереотипи про гендерні ролі, воно спрямоване проти людини через її гендерну приналежність і призводить до фізичної, сексуальної чи психологічної шкоди або страждань.

У цьому тексті ми будемо багато говорити про кіберзлочин та кіберпростір, тож пропонуємо визначення даних понять:

Кіберпростір (віртуальний простір) — середовище, яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Кіберзлочин — суспільно небезпечне діяння, яке вчиняється в кіберпросторі за допомогою спеціальних пристроїв, інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж тощо.

Необхідність проведення аналізу кіберзлочинів, пов'язаних із ГЗН, або гендерно зумовлених кіберзлочинів (далі - ГЗК), обумовлена кількома чинниками:

1. Зростання кількості випадків: Удосконалення комп'ютерних та інформаційних технологій призводить до появи нових форм насильства, які законодавець не встигає відобразити в законодавстві та надати дієві механізми протидії йому. Це створює ризики для безпеки, особливо жінок та дівчат, на яких спрямовується кібернасильство.

2. Недостатнє законодавче регулювання: В Україні питання кримінальної відповідальності за ГЗК, наразі не достатньо врегульоване. Відсутність чітких правових механізмів ускладнює притягнення винних до відповідальності та захист прав потерпілих.

3. Міжнародні зобов'язання: Ратифікація Стамбульської конвенції та отриман-

ня Загальної рекомендації ГРЕВІО №1 (детальніше про це у Розділі 2) зобов'язує Україну адаптувати своє законодавство до сучасних викликів кібернасильства та забезпечити ефективний захист прав людини в цифровому середовищі.

ГЗН у кіберпросторі може проявлятися у різних формах, наприклад:

- **Кібербулінг та кіберпереслідування:** Систематичне залякування, приниження чи погрози через цифрові платформи.
- **Розповсюдження інтимних матеріалів без згоди:** Публікація або поширення особистих фото чи відео сексуального характеру без згоди особи.
- **Онлайн-сталкінг:** Нав'язливе стеження за особою за допомогою цифрових засобів, збір та використання її персональних даних.
- **Сексуальні домагання в мережі:** Небажані коментарі, повідомлення чи контент сексуального характеру, спрямовані на приниження чи образу.

Ці форми кібернасильства не лише порушують права та свободи окремих осіб, але й підсилюють гендерні стереотипи та дискримінацію в суспільстві. Вони можуть мати серйозні психологічні наслідки для жертв, такі як тривога, депресія та навіть суїцидальні думки.

Розуміння природи та масштабів ГЗК є критично важливим для:

- **Розробки ефективного законодавства:** Необхідно створити правові механізми, які дозволять ефективно протидіяти кібернасильству та захищати права потерпілих.
- **Підвищення обізнаності суспільства:** Інформування громадськості про ризики та способи захисту від кібернасильства сприятиме зниженню кількості випадків та підтримці жертв.
- **Міжнародної співпраці:** Врахування міжнародного досвіду та рекомендацій допоможе Україні впровадити найкращі практики у сфері боротьби з кіберзлочинністю.

Цей звіт спрямований на аналіз поточного стану законодавчого регулювання кіберзлочинів, пов'язаних із гендерно зумовленим насильством в Україні, виявлення прогалин, що існують в чинному законодавстві та надання рекомендацій щодо їх усунення. Лише комплексний підхід дозволить ефективно протидіяти цьому негативному явищу та забезпечити захист прав кожної людини в цифровому просторі.

РОЗДІЛ 1:

ВИЗНАЧЕННЯ “КІБЕРЗЛОЧИНУ” В УКРАЇНСЬКОМУ ЗАКОНОДАВСТВІ

В сучасній Україні досить відомим є термін “кіберзлочин”, хоча в системі національного законодавства саме він не використовується.

Так що ж таке кіберзлочини й чи передбачено в Україні покарання за їх вчинення?

Для того, щоб розібратися в цьому питанні, проаналізуємо спочатку поняттєву базу, яка закріплена в нормативно-правових документах, а саме, в Кодексі України про адміністративні правопорушення¹ (далі - КУпАП) та Кримінальному кодексі України² (далі - КК України).

Так, положення КУпАП містять таке загальне визначення адміністративного правопорушення:

«Адміністративним правопорушенням (проступком) визнається протиправна, винна (умисна або необережна) дія чи бездіяльність, яка посягає на громадський порядок, власність, права і свободи громадян, на встановлений порядок управління і за яку законом передбачено адміністративну відповідальність.

Адміністративна відповідальність за правопорушення, передбачені цим Кодексом, настає, якщо ці порушення за своїм характером не тягнуть за собою відповідно до закону кримінальної відповідальності» (ст.9).

Чинні положення КУпАП містять кілька складів адміністративних правопорушень, які можна було б віднести до ГЗК, наприклад:

«Стаття 173-2. Вчинення домашнього насильства, насильства за ознакою статі, невиконання термінового заборонного припису або неповідомлення про місце свого тимчасового перебування

Вчинення домашнього насильства, насильства за ознакою статі, тобто умисне вчинення будь-яких діянь (дій або бездіяльності) фізичного, психологічного чи економічного характеру (застосування насильства, що не спричинило тілесних ушкоджень, погрози, образи чи переслідування, позбавлення житла, їжі, одягу, іншого майна або коштів, на

1 <https://zakon.rada.gov.ua/laws/show/80731-10#n60>

2 <https://zakon.rada.gov.ua/laws/show/2341-14#n1013>

які потерпілий має передбачене законом право тощо), внаслідок чого могла бути чи була завдана шкода фізичному або психічному здоров'ю потерпілого, а так само невиконання термінового заборонного припису особою, стосовно якої він винесений, або неповідомлення уповноваженим підрозділам органів Національної поліції України про місце свого тимчасового перебування в разі винесення такого припису».

«Стаття 173-4. Булінг (цькування) учасника освітнього процесу

Булінг (цькування), тобто діяння учасників освітнього процесу, які полягають у психологічному, фізичному, економічному, сексуальному насильстві, у тому числі із 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».

«Стаття 173-5. Мобінг (цькування) працівника

Вчинення мобінгу (цькування) працівника - тягне за собою накладення штрафу на громадян від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від двадцяти до тридцяти годин і накладення штрафу на фізичних осіб - підприємців, які використовують найману працю, посадових осіб - від ста до двохсот неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від тридцяти до сорока годин».

В зазначених вище статтях не обов'язково згадується окремо вчинення протиправних дій або бездіяльності за допомогою інформаційно-телекомунікаційних систем, але й не виключається, що підтверджується і судовою практикою, зокрема, у справах про вчинення булінгу.

Так, у Постанові Броварського міськрайонного суду Київської області від 12.10.2021 у справі №361/8716/21³ зазначено:

«ОСОБА_2 ... вчинив кібер булінг відносно учасника освітнього процесу ОСОБА_3 ... яке полягає у сексуальному насильстві, у тому числі із застосуванням засобів мобільного зв'язку ... а саме записав на свій мо-

3 <https://reyestr.court.gov.ua/Review/100897481>

більний телефон відеоролик сексуального характеру та розповсюдив його серед користувачів в мережі "Телеграм"...»

Також існує практика притягнення батьків малолітніх чи неповнолітніх, які чинять кібербулінг, до відповідальності за ч.1 ст.184 КУпАП «Невиконання батьками або особами, що їх замінюють, обов'язків щодо виховання дітей». І тут цікаво подивитися підбірку судових рішень одного і того ж суду:

«24.06.2023 року о 14:00 год. ОСОБА_1 в АДРЕСА_1 , ухилялася від виконання своїх батьківських обов'язків щодо виховання свого малолітнього сина ОСОБА_2 , 2010 року народження, який в зазначений час обробляв фото учениць Глинського ЗЗСО, підставляючи оголене тіло, та поширював в телеграм-каналі, принижуючи їхню честь та гідність...»

Постанова Жовківського районного суду Львівської області від 11.09.2023 у справі №444/3011/23⁴

«ОСОБА_1 24.06.2023 року о 14:00 год. в АДРЕСА_1 , ухилилася від виконання своїх батьківських обов'язків щодо виховання свого малолітнього сина ОСОБА_2 , 2010 року народження, який в зазначений час обробляв фото директора школи та однокласниць, підставляючи оголене тіло та поширював в телеграм-каналі, принижуючи їхню честь та гідність...»

Постанова Жовківського районного суду Львівської області від 13.09.2023 у справі №444/3054/23⁵

«ОСОБА_1 , ухиляється від виконання передбачених законодавством обов'язків щодо виховання свого малолітнього сина - ОСОБА_2 , 2010 року народження, що полягало в тому, що його малолітній син 24.06.2023 року близько 14 год. 00 хв. обробив фотографію свого класного керівника ОСОБА_3 , чим образив її честь та гідність...» -

Постанова Жовківського районного суду Львівської області від 05.10.2023 у справі №444/2898/23⁶

Своєю чергою, визначення кримінального правопорушення міститься в КК України:

4 <https://reyestr.court.gov.ua/Review/113340898>

5 <https://reyestr.court.gov.ua/Review/113409092>

6 <https://reyestr.court.gov.ua/Review/114276473>

«Кримінальним правопорушенням є передбачене цим Кодексом суспільно небезпечне винне діяння (дія або бездіяльність), вчинене суб'єктом кримінального правопорушення» (ч. 1 ст. 11).

Ознаками кримінального правопорушення є:

- **суспільна небезпечність** (спричинення шкоди об'єктам, що охороняються кримінальним законом, або реальна можливість заподіяння такої шкоди);
- **кримінальна протиправність** (кримінальним правопорушенням може бути визнано тільки таке суспільно небезпечне діяння, що передбачене кримінальним законом);
- **винність** (здійснення суспільно-небезпечного діяння у формі умислу чи необережності);
- **караність** (вчинення суспільно-небезпечного діяння передбачає відповідальність).

Тобто, коли ми використовуємо термін “кіберзлочин”, то говоримо про суспільно небезпечне діяння, яке вчиняється в кіберпросторі за допомогою спеціальних пристроїв, інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж тощо. А коли говоримо про скоєння такого злочину у кіберпросторі, то говоримо саме про середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Попри те, що питання кримінальної відповідальності за вчинення кримінальних правопорушень у цій сфері досить широко досліджувалися, зміст та особливості кримінальних правопорушень, які вчиняються у кіберпросторі й дотичні до ГЗН, наразі належним чином не досліджені та майже не відображені в чинному кримінальному законодавстві України.

На питання чому так склалося, можна відповісти дуже просто: *«завдяки удосконаленню комп'ютерних систем з'являються нові можливості для вчинення невідомих раніше правопорушень, а також традиційних злочинів новими засобами. Останнім часом в Україні наявна стійка тенденція до збільшення кількості злочинів, учинених у сфері використання електронно-обчислювальних машин (комп'ютерів; далі — ЕОМ), АС [автоматизованих*

систем] та комп’ютерних мереж і мереж електрозв’язку (комп’ютерних злочинів)»⁷.

Неймовірно швидкий розвиток сучасних цифрових та комп’ютерних технологій призводить до появи нових видів злочинів, які не відображені в кримінальному законодавстві.

Фактично, суспільство розвивається набагато швидше за правове регулювання певних питань, і можемо спостерігати за тим, що в ЗМІ вже досить часто використовуються певні визначення тих чи інших протиправних дій.

⁷ Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку [https://www.viaduk.net/clients/vsu/vsu.nsf/\(documents\)/AFB1E90622E4446FC2257B7C00499C02](https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02)

РОЗДІЛ 2:

**МІЖНАРОДНІ ВИЗНАЧЕННЯ КІБЕРЗЛОЧИНІВ ТА
КІБЕРНАСИЛЬСТВА ТА ЇХ РОЗУМІННЯ В УКРАЇНІ**

Першим міжнародним договором про кіберзлочини є **Конвенція про кіберзлочинність**⁸ (підписана у 2001 році, ратифікована Україною у 2005 році з набранням чинності 01.07.2006), метою якої є сприяння міжнародній співпраці в боротьбі з кіберзлочинами.

Цей документ регулює питання злочинів, пов'язаних з комп'ютерами, таких як:

- несанкціонований доступ до систем;
- несанкціоноване втручання в системи;
- фальсифікація даних та шахрайство;
- розповсюдження дитячої порнографії;
- порушення авторських прав через інтернет.

У 2016 році Радою з прав людини Генеральної Асамблеї ООН було сформульовано та закріплено в **Резолюції «Заохочення, захист та здійснення прав людини в Інтернеті»** від 01.07.2016 №32/13⁹ важливий підхід, що звучить наступним чином:

«ті самі права, які людина має в офлайновому середовищі, повинні також захищатися в онлайновому середовищі».

Спеціальний доповідач Ради ООН з прав людини з питань насильства стосовно жінок, його причин та наслідків, у своїй доповіді у 2018 році¹⁰ окремо проаналізував питання насильства в цифровій мережі та зазначив, поміж іншого, що:

- форми насильства щодо жінок в Інтернеті стають все більш поширеними у зв'язку з використанням соціальних мереж та інших технічних платформ (п. 12);
- завдяки легкому доступу та поширенню контенту в цифровому світі, соціальні, економічні, культурні та політичні структури, а також пов'язані з ними форми гендерної дискримінації та патріархальні моделі, які призводять до насильства за гендерною ознакою в офлайн-середовищі, відтворюються, а іноді посилюються та переосмислюються в інформаційно-комунікаційних технологіях, тоді як виникають і нові форми насильства (п. 20);

8 https://zakon.rada.gov.ua/laws/show/994_575#Text

9 <https://www.refworld.org/legal/resolution/unhrc/2016/en/112398>

10 <https://digitallibrary.un.org/record/1641160?v=pdf#record-files-collapse-header>

- Інтернет став простором для різних форм насильства над жінками й дівчатами, таких як порнографія, сексистські ігри та порушення права на приватність (п. 25);
- онлайн-насильство над жінками може проявлятися в різних формах і через різні засоби, зокрема в несанкціонованому доступі, використанні, поширенні приватних даних, інформації та/або контенту, фотографій та/або відео, в маніпуляціях або обміні ними, включно з сексуалізованими зображеннями, аудіокліпами та/або відео, або відредагованими за допомогою Photoshop (п. 34).

У 2022 році Європейським парламентом та Радою Європейського Союзу було прийнято **Регламент про єдиний ринок цифрових послуг** і внесення змін до **Директиви 2000/31/ЕС (Закон про цифрові послуги)**¹¹, яким поміж іншого було визначено:

«поняття “незаконний контент” слід визначати широко, щоб воно охоплювало інформацію, що стосується незаконного контенту, продуктів, послуг і діяльності. Зокрема, це поняття слід розуміти як посилання на інформацію, яка, незалежно від її форми, відповідно до чинного законодавства сама по собі є незаконною, як-от незаконна мова ворожнечі чи терористичний контент і незаконний дискримінаційний контент, або яка за чинними правилами вважається незаконною з огляду на те, що стосується незаконної діяльності. Ілюстративні приклади цього включають поширення зображень сексуального насильства над дітьми, незаконний обмін приватними зображеннями без згоди, переслідування в Інтернеті, продаж невідповідних або контрафактних продуктів, продаж продуктів або надання послуг із порушенням закону про захист прав споживачів, несанкціоноване використання захищеного авторським правом матеріалу, незаконні пропозиції послуг розміщення або незаконний продаж живих тварин. Натомість, відео очевидця потенційного злочину не слід вважати незаконним контентом лише тому, що воно зображує незаконну дію, якщо запис або розповсюдження такого відео для громадськості не є незаконним згідно з національним законодавством чи законодавством Союзу. У зв'язку з цим неважливо, чи є незаконність інформації чи діяльності наслідком законодавства Союзу чи національного законодавства, яке відповідає законодавству Союзу, і який точний характер або предмет закону, про який ідеться».

Також, питання кібернасильства висвітлені й у **Стратегії гендерної рівності Європейського Союзу на 2020-2025 роки**¹², зокрема, в її тексті зазначається:

¹¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014>

¹² <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0152>

«Всі мають бути в безпеці в своїх домівках, у своїх близьких стосунках, на своїх робочих місцях, у громадських місцях та в Інтернеті»;

«Насильство в Інтернеті, спрямоване на жінок, стало всеохопним із притаманними йому та жахливими наслідками; це неприпустимо. Це перешкода для участі жінок у суспільному житті. Залякування, переслідування та жорстоке поводження в соціальних мережах мають далекосяжні наслідки для повсякденного життя жінок і дівчат. ... Користувачі також мають бути здатні протистояти іншим видам шкідливого та образливого контенту, який не завжди вважається незаконним, але може мати руйнівні наслідки».

Важливим кроком виправлення ситуації, яка склалася в цій сфері, стало отримання Україною Загальної рекомендації ГРЕВІО (експертної групи з дій проти насильства стосовно жінок і домашнього насильства) № 1 щодо цифрового виміру насильства стосовно жінок¹³ (далі – Рекомендація) та ратифікація 20.06.2022 і подальше набрання чинності з 01.11.2022 **Конвенції Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами**¹⁴ (далі – Стамбульська конвенція), як еталон міжнародних стандартів у цій сфері.

Так, ГРЕВІО в тексті Рекомендації зазначено:

«На сьогодні не існує універсальної типології або визначення поведінки чи дій, які б об'єднували всі форми насильства стосовно жінок, вчинені в інтернеті або за допомогою технологій. Натомість, у дискурсах та підходах до насильницької поведінки в інтернеті та шкоди, заподіяної за допомогою технологій, використовуються взаємозамінні чи неточні терміни, створюючи фрагментацію, яка посилюється різноманітністю цілей і поглядів різних зацікавлених сторін, які наразі формують наратив. Багато термінів, які зараз використовуються, не охоплюють повного діапазону такої поведінки, а також не підкреслюють гендерну обумовленість насильства. Хоча вони й описують деякі дуже актуальні форми насильства стосовно жінок, які здійснюються в цифровому просторі, але не охоплюють усі види діяльності, що здійснюється в інтернеті або за допомогою технологій, які завдають шкоди жінкам і дівчатам».

Також у Рекомендації надано перелік термінів найпоширеніших форм цифрового насильства, наприклад:

¹³ <https://rm.coe.int/grevio-2021-20-first-general-recommendation-ukr/1680a4ad92>

¹⁴ https://zakon.rada.gov.ua/laws/show/994_001-11#Text

- **аутинг** - розкриття сексуальної орієнтації чи ґендерної ідентичності особи без її згоди, часто публічно;
- **бодішеймінг** - коментування та висміювання чиєїсь форми тіла, розміру одягу чи зовнішності;
- **деднейминг** - свідоме використання паспортного імені, яке було при народженні (і не відповідає ґендеру особи), щоб присоромити, погрозити, налякати чи образити особу;
- **діпфейки** - відео, у яких одне обличчя (повністю та бездоганно) замінено іншим обличчям за допомогою алгоритмів і глибинного навчання, а звуком маніпулюють так, щоб створити ілюзію того, що було знято дії іншої особи;
- **доксинг** - поширення особистої інформації цільової особи в інтернеті я особистої інформації цільової особи в інтернеті (номер телефону, адреса електронної пошти, домашня адреса, професійні контакти) без її згоди з метою заохочення насильства;
- **кібернасильство, кібербулінг** - знущання, яке відбувається за допомогою цифрових інструментів та оточення, яке зазвичай розуміється як залякування неповнолітніх;
- **кіберфлешинг** - надсилання небажаних зображень сексуального характеру через додатки для знайомств або обміну повідомленнями, за допомогою текстових повідомлень або технологій Airdrop чи Bluetooth;
- **кріпшоти** - світлини жінок сексуального характеру, виготовлені без їхньої згоди;
- **орбітинг** - особа не відповідає на повідомлення або не спілкується з іншою особою безпосередньо, але продовжує переглядати її контент в інтернеті (ставить лайки, переглядає сторіс тощо);
- **приглушення** - неспроможність особи повноцінно брати участь і висловлювати себе в інтернеті через страх перед насильством, що в кінцевому підсумку призводить до виключення такої особи з публічних обговорень, у яких вона хотіла б брати участь;
- **“радісне побиття” (знятий напад)** - це напад (фізична атака або сексуальний напад) на жертву, який записується на камеру для подальшого поширення в інтернеті;
- **сватинг** - використання телефонів і часто комп’ютерних систем для введення служби екстреної допомоги в оману так, щоб правоохоронні органи за хибним повідомленням виїхали за адресою іншої особи;

- **секстинг** - обмін, надсилання або отримання повідомлень сексуального характеру, які часто містять зображення або відео, за допомогою текстових повідомлень або чату;
- **сексуальне вимагання** - використання загрози опублікувати контент сексуального характеру (зображення, відео, діпфейки, чутки про сексуальне життя) для залякування, примусу чи шантажу особи, щоб отримати ще більше контенту сексуального характеру або щоб отримати гроші, іноді й те, й інше;
- **сексуальне насильство на основі зображень** - кривдник отримує зображення або відео відверто сексуального характеру під час стосунків, або зламує чи викрадає їх із комп'ютера, облікових записів у соціальних мережах чи з телефону жертви, щоб поширити їх в інтернеті;
- **тролінг** - це свідоме публікування образливих коментарів в інтернеті, іноді з наявним наміром викликати тривогу, переживання або приниження. Такі атаки також можуть здійснюватися групою людей у скоординований та цілеспрямований спосіб.
- **флейминг** - розміщення образливих або ворожих повідомлень, включно з образами, у соціальних мережах або на форумах;

Цікаво, що всупереч відсутності законодавчого закріплення даних визначень, у деяких текстах судових рішень (у кримінальних справах) їх можна знайти, хоча (в деяких випадках) не в зовсім вірному використанні, наприклад:

«ОСОБА_3 звернулась до слідчого судді із вказаною скаргою, мотивуючи тим, що 26 березня 2021 року вона подала до Департаменту кіберполіції НП України заяву про вчинення злочину -кібербулінгу (розповсюдження порнографічного контенту з її обличчям в мережі Інтернет, намагання втягнути до проституції та вимагання коштів за не розповсюдження порнографічного контенту з її обличчям в мережі Інтернет)».

Ухвала Жовтневого районного суду міста Кривого Рогу Дніпропетровської області від 23.04.2021 у справі №212/3032/21¹⁵

«Розслідується кримінальне провадження за відомостями про вчинення адміністраторами каналу месенджеру "Telegram" під назвою "Николаев отбросы, и сущности НОМЕР_5" кібербулінгу, цькування відносно жителів м. Миколаєва, а також розміщення матеріалів образливого

15 <https://reyestr.court.gov.ua/Review/96528540>

характеру з ціллю шантажування малолітніх осіб та отримання з них грошових коштів за видалення таких матеріалів».

Ухвала слідчого судді Центрального районного суду м. Миколаєва від 02.08.2024 у справі №490/6347/24¹⁶

«Стосовно інформації з телеграм-каналів, захисник вважає, що її неможливо визнати допустимим доказом, оскільки публікувати її може будь-хто із будь-якою невстановленою метою, створювати діпфейки та ін. Телеграм канали не є офіційним джерелом інформації».

Вирок Запорізького апеляційного суду від 14.05.2024 у справі №333/3237/23¹⁷

«Також взято до уваги інформацію, наведену прокурором щодо особи та діяльності ініціатора скарги ОСОБА_4, яку підтвердив із офіційних джерел у мережі інтернет, а саме із сайту Вікіпедії та додав у друкованому вигляді, що ГО "НОН-СТОП" займається медійними та юридичними атаками на комерційні структури, окремих осіб та державні установи в інтересах замовників та процесуальним тролінгом, що включає у себе публікацію на сторінках ГО у соціальних мережах із звинуваченням, потім подача заяв про "злочин" і відкриття через суд кримінального провадження проти об'єкта атаки, отримання відповідей від правоохоронців, витягів із ЄРДР і монтаж підсумкового відео з дискредитацією об'єкта атаки».

Ухвала слідчого судді Придніпровського районного суду м. Черкаси від 15.03.2024 у справі №711/2088/24¹⁸

«Досудовим розслідуванням встановлено, що 05.10.2022 до Дарницького УП ГУ НП у м. Києві надійшло повідомлення з Департаменту кіберполіції стосовно вчинення невстановленими особами незаконного втручання в роботу автоматизованих електронно-обчислювальних машин.

Так встановлено, що в червні місяці (більш точну дату досудовим розслідуванням не встановлено) гр. ОСОБА_6 відносила свій мобільний телефон для ремонту до майстра за адресою: м. Київ, пр-т Соборності, 17. Де майстер підключав телефон до комп'ютера та мав доступ до всіх

16 <https://reyestr.court.gov.ua/Review/121269950>

17 <https://reyestr.court.gov.ua/Review/119362729>

18 <https://reyestr.court.gov.ua/Review/117689538>

медіа та фото, а також до iCloud.

Після чого 27.09.2022 ОСОБА_6 отримала повідомлення від невстановленої досудовим розслідуванням особи у месенджері «Телеграм» на англійській мові, з приводу того що вона володіє особистими фото та відео інтимного характеру ОСОБА_6, з iCloud., та в підтвердження чого надіслала вказані фото та відео матеріали, а також повідомила що за нерозповсюдження даних фото та відео друзям та батькам ОСОБА_6, остання повинна відправити 200 доларів США на номер телефону...»

Ухвала слідчого судді Дарницького районного суд м.Києва від 06.02.2023 у справі № 753/546/23¹⁹

«Суд враховує, що зазначений текст, шляхом репосту (“поділитися темою, публікацією” був подалі розповсюджений ОСОБА_7 у соціальній мережі “Однокласники” без будь-якого коментаря з її боку. При цьому, сама по собі дія “поділитися темою, публікацією” - не може бути однозначною ознакою підтримки її змісту. Функція “Поділитися темою, публікацією” у інтернет-спільноті соціальних мереж розуміється, як підтримка теми, або запрошення на обговорення, або має меті тролінг, тощо».

Вирок Іллічівського міського суду Одеської області від 31.05.2021 у справі №501/1321/20²⁰

Такі випадки також підтверджують необхідність найшвидшого реагування законотворчих органів з метою внесення змін до чинного законодавства.

Окремо варто зупинитися на Стамбульській конвенції, яка базується на чотирьох головних принципах: **запобігання, захист, переслідування та скоординована політика**. У ній закріплено необхідність вживати заходів, зокрема, для:

- «забезпечення того, щоб умисну поведінку, яка призводить до тяжкого порушення психічної цілісності шляхом примушування або погроз, було криміналізовано» (стаття 33);
- «забезпечення того, щоб умисну поведінку, яка полягає в повторному здійсненні загрозливої поведінки, спрямованої на іншу особу, що змушує його чи її боятися за свою безпеку, було криміналізовано»

¹⁹ <https://reyestr.court.gov.ua/Review/108795516>

²⁰ <https://reyestr.court.gov.ua/Review/97301758>

(стаття 34);

- «забезпечення того, щоб будь-яка форма небажаної вербальної, не-вербальної або фізичної поведінки сексуального характеру, метою або наслідком якої є порушення гідності особи, зокрема шляхом створення залякувального, ворожого, принизливого або образливого середовища, підлягала кримінальній або іншій юридичній санкції» (стаття 40).

Також Стамбульська конвенція покладає на державу обов'язок вжиття *“необхідних законодавчих або інших заходів для забезпечення того, щоб насильство стосовно жінок за гендерною ознакою могло бути визнано як форма переслідування”* (стаття 60).

Зазначені вище вимоги та загальний напрямок руху України до отримання членства в Євросоюзі призводять, хоча й повільно, до поступових змін в національному законодавстві.

При цьому певна неузгодженість наявного законодавства, зміни до якого недостатньо швидко вводяться в площину законодавчого регулювання, та недостатнє висвітлення ефективних дій правоохоронної системи в площині ГЗК призводять до певної недовіри серед суспільства.

Моніторинг відкритих джерел показує, що суспільство реагує на такі кіберзлочини, описує їх, але не звертається за допомогою до правоохоронних органів:

- у 2021 році в мережі з'явилася інформація про розповсюдження інтимних зображень без згоди особи²¹ – колишній хлопець надіслав оголені фото жінки в чат з колегами. *«Я беру телефон, відкриваю Telegram і бачу сповіщення з робочого чату з попередньої роботи, де ми з колишнім познайомилися. Це чат на приблизно 50 людей ... Я відкриваю чат – і бачу себе на фото. Голу. Видно груди, геніталії – все. Таких фото десь п'ять або шість. Спочатку я не розумію, що відбувається, стою у ступорі. Серце падає в п'ятки. Кидає в жар. Ще раз перевіряю, що це за чат, і ще раз передивляюсь фотографії. Складно дихати. Мене починає нудити. 50 людей бачили мене повністю голою.»*.

Опис ситуації дає підстави вважати, що жінка не звернулася до правоохоронних органів, а лише видалила фото в себе і зазначила *«...На жаль, ні в кого з них немає прав на те, щоб видалити їх із чату повністю, тому в деяких людей вони, можливо, є й досі.»*.

- у 2023 році відома виконавиця Jerry Heil у своєму Telegram артистка розповіла,

21 <https://www.village.com.ua/village/city/city-experience/312649-pornopomsta>

що житель країни-агресорки надокучає їй в соціальних мережах та надсилає образливі повідомлення. Співачка, розуміючи протиправність таких дій, звернулася за допомогою до поліції, однак **“правоохоронці не виявили жодних порушень”**²².

Варто зазначити, що і звернення до поліції з повідомленнями про вчинення кібернасильства не завжди стають підставою для притягнення до відповідальності саме винної особи.

Така ситуація проілюстрована інформацією, яка міститься в Постанові Голосіївського районного суду міста Києва від 09.08.2022 у справі 752/8879/22²³. Батько малолітньої дівчини звернувся до поліції з інформацією, що його донька розповіла йому про те, що «в мережі інтернет познайомилася з невідомим чоловіком, якому переслала своє напівоголене зображення. Після цього цей чоловік став переписуватися з нею у месенджері “телеграм”, вимагати інші фотографії інтимного змісту, наполягати на зустрічі та вів мову про вступ в інтимні стосунки. Злякавшись того, що відбувається [донька] звернулася до батька для захисту».

Поліція, отримавши зазначену інформацію, замість відкриття кримінального провадження та вчинення дій по розшуку невідомого, який переслідував малолітню дитину, склала протокол на її батька за адміністративне правопорушення за ч. 1 ст. 184 КУпАП “Невиконання батьками або особами, що їх замінюють, обов’язків щодо виховання дітей”.

²² <https://tsn.ua/glamur/jerry-heil-peresliduye-neadekvatniy-rosiyanin-do-viyni-priyihav-do-lvova-2357284.html>

²³ <https://reyestr.court.gov.ua/Review/105669828>

РОЗДІЛ 3:

ПРАКТИКИ ЗАСТОСУВАННЯ В УКРАЇНІ

Законом України “Про основні засади забезпечення кібербезпеки України”, прийнятим 05.10.2017, визначено, що серед об’єктів кібербезпеки є конституційні права і свободи людини й громадянина (ст. 4), забезпечення кібербезпеки в Україні ґрунтується, в тому числі, на принципі верховенства права, законності, поваги до прав людини й основоположних свобод та їх захисту (ст. 7) та встановлена відповідальність за кіберзлочини (ст. 12).

Цим же законом закріплено і термінологічний блок – наприклад, таке: **«кіберзлочином** (комп’ютерним злочином) визначається «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» та визначення **кіберпростору**, яке було згадано вище.

В чинній (на дату підготовки даного звіту) редакції КК України є склади кримінальних правопорушень, які можуть бути віднесені до ГЗН та можуть бути визначені, як кіберзлочини, наприклад:

Стаття 156-1. Домагання дитини для сексуальних цілей.

«1. Пропозиція зустрічі, зроблена повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, особі, яка не досягла шістнадцятирічного віку, з метою вчинення стосовно неї будь-яких дій сексуального характеру або розпусних дій, у разі якщо після такої пропозиції було вчинено хоча б одну дію, спрямовану на те, щоб така зустріч відбулася.

2. Пропозиція зустрічі, зроблена повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, неповнолітній особі з метою втягнення її у виготовлення дитячої порнографії, якщо після такої пропозиції було вчинено хоча б одну дію, спрямовану на те, щоб така зустріч відбулася».

Стаття 161. Порушення рівноправності громадян залежно від їх расової, національної, регіональної належності, релігійних переконань, інвалідності та за іншими ознаками. *«Умисні дії, спрямовані на розпалювання національної, регіональної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або об-*

раза почуттів громадян у зв'язку з їхніми релігійними переконаннями, а також пряме чи непряме обмеження прав або встановлення прямих чи непрямих привілеїв громадян за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, інвалідності, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками».

Стаття 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер. «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер».

Стаття 182. Порушення недоторканності приватного життя. «Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу».

Стаття 189. Вимагання. «Вимога передачі чужого майна чи права на майно або вчинення будь-яких дій майнового характеру з погрозою насильства над потерпілим чи його близькими родичами, обмеження прав, свобод або законних інтересів цих осіб, пошкодження чи знищення їхнього майна або майна, що перебуває в їхньому віданні чи під охороною, або розголошення відомостей, які потерпілий чи його близькі родичі бажають зберегти в таємниці (вимагання)».

Стаття 301-1. Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження. «Умисне одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем чи технологій або умисне її придбання, або умисне зберігання, ввезення в Україну, перевезення чи інше переміщення дитячої порнографії без мети збуту чи розповсюдження».

Стаття 301-2. Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи.

- «1. Проведення видовищного заходу сексуального характеру, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому задіяно неповнолітню особу
2. Відвідування видовищного заходу сексуального характеру з метою його перегляду, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому завідомо для відвідувача задіяно малолітню чи неповнолітню особу
3. Втягнення неповнолітньої особи до участі у видовищному заході сексуального характеру, що проходить, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, або примушування неповнолітньої особи до участі у такому заході з використанням обману, шантажу, уразливого стану особи або із застосуванням чи погрозою застосування насильства».

Проте, КК містить в собі й ряд складів кримінальних правопорушень, які можуть відноситися до ГЗН, але їх диспозиція не передбачає, що вони можуть бути кіберзлочинами, наприклад:

Стаття 120. Доведення до самогубства. «Доведення особи до самогубства або до замаху на самогубство, що є наслідком жорстокого з нею поводження, шантажу, систематичного приниження її людської гідності або систематичного протиправного примусу до дій, що суперечать її волі, схиляння до самогубства, а також інших дій, що сприяють вчиненню самогубства».

Стаття 126-1. Домашнє насильство. «Домашнє насильство, тобто умисне систематичне вчинення фізичного, психологічного або економічного насильства щодо подружжя чи колишнього подружжя або іншої особи, з якою винний перебуває (перебував) у сімейних або близьких відносинах, що призводить до фізичних або психологічних страждань, розладів здоров'я, втрати працездатності, емоційної залежності або погіршення якості життя потерпілої особи».

Стаття 127. Катування. «Катування, тобто будь-яке умисне діяння, спрямоване на заподіяння особі сильного фізичного болю чи морального страждання, вчинене з метою примусити її чи іншу особу вчинити дії, що суперечать їх волі, у тому числі отримати інформацію чи зізнання, або з метою покарати її чи іншу особу за дії, вчинені нею або іншою особою чи у вчиненні яких вона або інша особа підозрюється, або з метою залякування її або інших осіб».

Стаття 129. Погроза вбивством. «Погроза вбивством, якщо були реальні підстави побоюватися здійснення цієї погрози».

Вибірковий моніторинг Єдиного державного реєстру судових рішень (далі - ЄДРСР) показує, що в провадженні національних судів перебували справи за деякими вищевказаними статтями та, в певних випадках, мотивувальні частини судових рішень містили описову частину кіберзлочинів:

“Неповнолітня потерпіла ...в судовому засіданні ... пояснила, що ... Обвинувачений неодноразово погрожував, що розповсюдить її фотознімки інтимного характеру, а тому вона протягом певного періоду боялась розповісти про події своїм рідним...”

*Вирок Народицького районного суду Житомирської області
у справі №284/453/2²⁴*

За результатами розгляду справи, обвинуваченого було визнано винним у вчиненні злочинів, передбачених частиною 1 статті 155 (Вчинення дій сексуального характеру з особою, яка не досягла шістнадцятирічного віку), частиною 1 статті 156 (Розбещення неповнолітніх), частиною 1 статті 156-1 (Домагання дитини для сексуальних цілей) КК України.

«ОСОБА_4 в період часу з 02 по 24 квітня 2018 року, з метою помсти ОСОБА_7 ... через розлучення із нею ... без згоди ОСОБА_7 ... поширив раніше знятий ним в липні 2016 року відеозапис ... на яких демонструються оголені статеві органи та процес природного статевого акту та неприродного (орогенітального) контакту між ним - ОСОБА_4 та його на той час дружиною ОСОБА_7 ... чим порушив право потерпілої ОСОБА_7 ... на недоторканість приватного життя.»

*Вирок Миколаївського районного суду Львівської області,
у справі №447/105/19²⁵*

За результатами розгляду справи, обвинуваченого було визнано винним у вчиненні злочину, передбаченого ч. 1 ст. 182 (Порушення недоторканності приватного життя) та ст. 301 ч. 2 (Ввезення, виготовлення, збут і розповсюдження порнографічних предметів) КК України.

²⁴ <https://reyestr.court.gov.ua/Review/107243051>

²⁵ <https://reyestr.court.gov.ua/Review/79798221>

«Свідок ... в судовому засіданні показала, що у вересні 2022 року обвинувачений ... написав їм у групу Інстаграм повідомлення: чи хочете побачити "пушку". Вона та інші однокласники створили на його прохання групу в мобільному телефоні "Телеграм", куди він скинув два відео, на яких були зображення непристойного характеру за його участю та участю потерпілої, їх однокласниці ... Окрім показів свідків, допитаних у справі, вина ... у вчиненні інкримінованого йому діяння стверджена дослідженими в судовому засіданні матеріалами кримінальної справи: ... протоколами огляду предмета - мобільного телефона обвинуваченого ... в якому містилися відеофайли порнографічного характеру за участю обвинуваченого ... та потерпілої ... а також переписка між ними, в якій містяться погрози оприлюднити їх у соціальних мережах...»

Вирок Іршавського районного суду Закарпатської області у справі №447/105/19²⁶

За результатами розгляду справи, обвинуваченого було визнано винним у вчиненні злочину, передбаченого ч. 3 ст. 301-1 (Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження) КК України.

Звісно, що ситуація з законодавчим врегулюванням зазначених вище питань не ідеальна, але вона поступово змінюється на краще, хоча й досить повільно.

Так, 22.05.2024 Верховною Радою України було прийнято Закон України "Про внесення змін до Кодексу України про адміністративні правопорушення та інших законів України у зв'язку з ратифікацією Конвенції Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу з цими явищами"²⁷, який набирає чинності 19.12.2024 та доповнює КУпАП новою статтею, яка містить в собі частину, що стосується кіберзлочину, в цьому випадку, адміністративного правопорушення:

Стаття 173-7. Сексуальне домагання «Сексуальне домагання, тобто умисне вчинення проти бажання особи образливих, принизливих дій сексуального характеру, виражених вербально або невербально (слова, жести, рухи тіла), у тому числі з використанням електронних комунікацій».

²⁶ <https://reyestr.court.gov.ua/Review/114467778>

²⁷ <https://zakon.rada.gov.ua/laws/show/3733-20#Text>

Також позитивним прикладом може бути й законопроект №12088²⁸, зареєстрований у Верховній Раді України 03.10.2024, яким запропоновано внести зміни у ч. 1 ст. 1 до Закону України “Про запобігання та протидію домашньому насильству”, додавши нові пункти такого змісту:

*«6) **злочинне переслідування (сталкінг)** – форма психологічного домашнього насильства, яка виражається у небажаній нав’язливій увазі до однієї людини з боку іншої людини або групи людей, а також полягає у стеженні за постраждалою особою та неодноразовому перебуванні біля місця її проживання;*

*7) **кіберпереслідування** – вид злочинного переслідування, що передбачає постійне спостереження за постраждалою особою без її згоди чи законного дозволу за допомогою інформаційних та комунікаційних технологій, що може здійснюватися шляхом обробки персональних даних жертви, зокрема в результаті крадіжки особистих даних або шпигування за жертвою через її соціальні мережі або платформи обміну повідомленнями, електронну пошту та телефон, крадіжку паролів або злом її пристроїв для доступу до приватного простору за допомогою встановлення додатків геолокації, у тому числі шпигунського програмного забезпечення, або через викрадення її пристроїв».*

В пояснювальній записці до даного законопроекту, зокрема, зазначено наступне:

«Щороку від насильства в Україні потерпає близько 200 тисяч осіб. Серед них 90% жінок. Зокрема, згідно отриманих від Міністерства соціальної політики України статистичних даних про загальну кількість випадків домашнього насильства за період з 2017-го по 2023 рік чітко проглядається, що динаміка випадків вчинення домашнього насильства тільки зростає, так протягом 2017 року зареєстровано - 96 606 звернень, 2018 рік – 106 549 таких звернень, 2019 рік – 130 514, 2020 рік – 211 362, 2021 рік – 284 221, 2022 рік – 251 829, 2023 рік – 251 954.

Згідно отриманих даних від Національної поліції України за період 2017–2023 про кількість складених органами поліції протоколів про адміністративні правопорушення, передбачені статтею 173-2 КУпАП (Вчинення домашнього насильства, насильства за ознакою статі, невиконання термінового заборонного припису або неповідомлення про місце свого тимчасового перебування), свідчить про наявну тенденцію до їх

28 <https://itd.rada.gov.ua/billInfo/Bills/Card/44972>

збільшення у порівнянні з минулими роками (2017 рік – 91 974 адмін-протоколів, 2018 – 101 699, 2019 рік – 109 332, 2020 рік – 133 690, 2021 рік – 147 017, 2022 рік – 120 533, 2023 рік – 163 542).

Відсутність законодавчого регулювання поняття “сталкінгу” в Україні обумовлює актуальність законодавчого врегулювання даного питання».

Варто зауважити, що такі позитивні зміни не стосуються ситуацій, з якими стикаються ЛГБТКІ+ люди, оскільки ні в КК, ні в КУпАП України не закріплено окремо такі захищені ознаки, як сексуальна орієнтація та гендерна ідентичність.

Тобто, будь-яка форма цифрового насильства, вчинена стосовно представників ЛГБТ-КІ+ спільноти через їх приналежність до неї, не буде належним чином враховуватися без додаткових аргументів.

Єдиним належним шляхом виправлення цієї ситуації може бути внесення відповідних змін до законодавства, але реальних кроків у цьому напрямку держава не зробила, хоча є певні спроби.

Так, ще 13.05.2021 у Верховній Раді України було зареєстровано законопроект №5488²⁹ про внесення змін до Кодексу України про адміністративні правопорушення та Кримінального кодексу України щодо боротьби з проявами дискримінації, яким, зокрема, передбачено закріплення в переліку захищених ознак сексуальної орієнтації та гендерної ідентичності, а також введення відповідальності за розпалювання ворожнечі та ненависті на ґрунті нетерпимості, в тому числі за *“публічні заклики до насильства на ґрунті нетерпимості, а також інші умисні дії, спрямовані на розпалювання ворожнечі та ненависті на ґрунті нетерпимості”*.

Даний законопроект досі перебуває тільки на стадії отримання висновків комітетів Верховної Ради України.

29 https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=71891

РОЗДІЛ 4:

ПРАКТИКА ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ

Окремо варто зупинитися і на практиці Європейського суду з прав людини (далі – ЄСПЛ), рішення якого є обов’язковими для виконання Україною, враховуючи приписи Закону України “Про виконання рішень та застосування практики Європейського суду з прав людини”³⁰.

Так, однією з перших справ, в якій ЄСПЛ здійснював аналіз **Європейської конвенції з прав людини**³¹ (далі – Конвенція) в контексті кібернасильства, стала справа K.U. v. FINLAND (Заява №2872/02)³², в якій досліджувалося питання розміщення оголошення сексуального характеру на інтернет-сайті знайомств від імені заявника, якому було дванадцять років, без його відома.

Заявник зазначав, що законодавство Фінляндії у період, про який йдеться у справі, захищало злочинця, тоді як потерпілий не мав засобів для отримання відшкодування чи захисту проти порушення приватності (§46).

ЄСПЛ, надаючи оцінку доводам сторін, встановив порушення ст. 8 Конвенції та зазначив,

«що практичний та дієвий захист заявника вимагав вжиття дієвих кроків для ідентифікації та кримінального переслідування порушника, тобто особи, яка розмістила оголошення. У цій справі такий захист не був наданий. Ефективне розслідування в жодному разі не могло бути розпочато через переважаючу вимогу конфіденційності. Хоча свобода вираження поглядів та конфіденційність комунікацій є надзвичайно важливими, а користувачі телекомунікаційних та інтернет-послуг повинні мати гарантію, що їхня приватність та свобода вираження поглядів буде поважатися, така гарантія не може бути абсолютною і в окремих випадках повинна поступатися іншим правомірним вимогам, таким як запобігання заворушенням чи злочинам або захист прав і свобод інших осіб. Не упереджуючи питання того, чи можуть дії особи, яка розмістила неналежне оголошення в інтернеті, підлягати захисту за статтями 8 та 10, враховуючи природу цього оголошення, що варта осуду, все ж завданням законодавця є створити механізми для узгодження різних вимог, які конкурують за захист у цьому контексті. Такі механізми, проте, були відсутні на момент подій у справі, що призвело до того,

30 <https://zakon.rada.gov.ua/laws/show/3477-15#Text>

31 https://zakon.rada.gov.ua/laws/show/995_004#Text

32 [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-89964%22](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-89964%22)

що позитивний обов'язок Фінляндії по відношенню до заявника не міг бути реалізований...» (§49).

Інша справа, яка розглядалася ЄСПЛ і є прикладом розповсюдження інтимних зображень та фото без згоди особи – це справа KHADIJA ISMAYILOVA v. AZERBAIJAN (Заява №65286/13 та №57270/14)³³, у якій заявниця, відома опозиційна журналістка-розслідувачка, отримала лист, що містив зображення з прихованої камери, встановленої у її спальні, на яких було зафіксовано статевий акт між нею та її колишнім хлопцем. У повідомленні до цих зображень містився текст: *«Повія, утримайся від того, що ти робиш, інакше тобі буде ганьба»*. Такі самі листи були направлені й двом опозиційним газетам.

ЄСПЛ, надаючи оцінку доводам сторін, встановив порушення ст. 8 Конвенції та зазначив, що вчинені відносно заявниці дії на перший погляд здавалися результатом ретельно спланованої та проведеної операції за участю скоординованих зусиль кількох осіб (§121).

При цьому, хоча твердження заявниці стосовно того, що представники держави могли стояти за кримінальним правопорушенням, вчиненим проти неї, не підтверджені доказами, її аргументи в цьому відношенні були сильними й не могли бути відкинуті як неспроможні на перший погляд, та вимагали від розслідування пошуку доказів, що підтвердили б даний факт (§122).

Також ЄСПЛ відзначив відсутність інформації про проведення відповідних слідчих дій стосовно встановлення власників та/або операторів вебсайтів, на яких були розміщені відео з заявницею, з метою визначення джерел відео та осіб, які їх завантажити вперше (§127).

Також уваги заслуговує і справа BUTURUGĂ v. ROMANIA (Заява №56867/15), у якій вперше було досліджено та оцінено кібербулінг як форму насильства над жінками.

Заявниця у справі стверджувала, що звернулася до органів влади своєї країни з заявами про те, що її колишній чоловік здійснював відносно неї насильницькі дії, незаконно отримав доступ до її електронних облікових записів, у тому числі у Facebook, зробив копії її приватних розмов, документів і фотографій. За результатами розгляду її звернення, кримінальне провадження було закрито у зв'язку з відсутністю загрози суспільної без-

33 [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-188993%22}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-188993%22})

пеки, натомість колишнього чоловіка притягнули до адміністративної відповідальності.

ЄСПЛ за результатом розгляду даної справи винес рішення про порушення статей 3 та 8 Конвенції та зазначив, що розгляд справ про домашнє насильство потребує особливої ретельності та прийняття до уваги контексту домашнього насильства (§67).

Також ЄСПЛ прийняв аргументи заявниці про те, що такі дії, як незаконний моніторинг, збереження кореспонденції партнера або доступ до неї, можуть бути взяті до уваги національними органами під час розслідування справ про домашнє насильство. Він відзначив, що згідно з національним і міжнародним правом явище домашнього насильства не розглядається як таке, що обмежується одним лише фактом фізичного насильства, а вважається таким, що включає, серед інших аспектів, психологічне насильство та переслідування. Крім того, наразі кіберзалякування визнано одним з аспектів насильства щодо жінок і дівчат, що може приймати різноманітні форми, такі як порушення кіберприватності, вторгнення в комп'ютер жертви та захоплення, обмін і маніпулювання даними та зображеннями, у тому числі особистими даними (§74).

РОЗДІЛ 5:

ПРОЦЕДУРА ВНЕСЕННЯ ВІДОМОСТЕЙ ДО ЄРДР

Наразі в Україні існує єдина система реєстрації кримінальних правопорушень, яка регулюється окремими положеннями Кримінального процесуального кодексу України³⁴ (далі - КПК України), наказом Офісу Генерального прокурора від 30.06.2020 N298 "Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення" та Наказом МВС України від 08.02.2019 N100 "Про затвердження Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події".

Єдиний реєстр досудових розслідувань (далі - ЄРДР) - це електронна система, яка зберігає інформацію щодо досудових розслідувань і кримінальних справ.

Положенням про ЄРДР, порядок його формування та ведення³⁵ визначено, що власником і розпорядником ЄРДР є держава в особі Офісу Генерального прокурора, а реєстраторами (уповноваженими особами, які створюють (редагують) інформацію (електронні форми) про кримінальні правопорушення) є прокурори, керівники органів прокуратури, керівники органів досудового розслідування та органів дізнання, слідчі та дізнавачі.

Статтею 214 КПК України визначено, що досудове розслідування розпочинається з моменту внесення відомостей до ЄРДР, а внесення інформації до даного реєстру здійснюється слідчим, дізнавачем або прокурором *«невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення...»*

Ба більше, відповідно до положень ч. 4 ст. 214 КПК України, відмова у прийнятті та реєстрації заяви чи повідомлення про кримінальне правопорушення не допускається, а уповноважені на прийняття та реєстрацію заяв і повідомлень про кримінальні правопорушення зобов'язані прийняти та зареєструвати таку заяву чи повідомлення.

Тобто, право внесення інформації про кримінальні правопорушення закріплено за чітко визначеними процесуальними особами: слідчим, дізнавачем або прокурором, і повинно виконуватися безумовно, оскільки перевірка викладених в заявах та повідомленнях фактів про вчинене кримінальне правопорушення здійснюється у порядку досудового розслідування, і, коли відсутній склад або подія злочину, кримінальне провадження

³⁴ <https://zakon.rada.gov.ua/laws/show/4651-17#n2036>

³⁵ <https://zakon.rada.gov.ua/laws/show/v0298905-20#n790>

підлягає закриттю.

Попри це, є непоодинокі випадки, коли заяви, повідомлення про вчинене кримінальне правопорушення, які містять відомості про кримінальне правопорушення, не вносяться уповноваженими особами до ЄРДР одразу.

Така практика може призводити до втрати досить великого обсягу інформації про кіберзлочини, оскільки не всі заявниці мають правові знання щодо можливості оскарження невнесення відомостей до ЄРДР та строків такого оскарження.

Це стосується і ГЗК, інформація про які вноситься до ЄРДР за ухвалою слідчого судді. Зазначене вище може мати відображення в деяких судових рішеннях, які містяться в ЄДРСР:

1. Справа №466/189/22, яка 13.01.2022 була розглянута слідчим суддею Шевченківського районного суду м. Львова³⁶.

У цій справі скаржниця звернулася до слідчого судді зі скаргою на дії посадових осіб щодо невнесення відомостей до ЄРДР та зазначила, що *«11.11.2021 о 09:30 год. вона звернулась до Управління протидії кіберзлочинам у Львівській області Департаменту кіберполіції Національної поліції України з усним повідомленням про вчинення відносно неї кримінального правопорушення.*

Суть повідомлення, як зазначила скаржник, полягала в тому, що невідома особа в період часу з 24.10.2021 по день її звернення, незаконно заволоділа та розпоряджалася її персональними даними, втручалася в її особисте життя, розмістивши від її імені оголошення про надання інтимних послуг, компроментуючи її перед її близькими та знайомими, принижуючи її честь та гідність. ...

Проте її повідомлення не було внесено до ЄРДР.»

Слідчий суддя, розглянувши матеріали справи, зобов'язав уповноважених осіб внести відомості про кримінальне правопорушення до ЄРДР на підставі повідомлення особи про вчинення кримінального правопорушення та розпочати розслідування.

2. Справа №212/5558/21, яка 05.07.2021 була розглянута слідчим суддею Жовтневого районного суду міста Кривого Рогу Дніпропетровської області³⁷.

Скаржниця звернулася до слідчого судді зі скаргою на дії посадових осіб щодо невнесення відомостей до ЄРДР та зазначила, що *«вона звернулася до ВП №3 КРУП*

³⁶ <https://reyestr.court.gov.ua/Review/102662758>

³⁷ <https://reyestr.court.gov.ua/Review/98134741>

ГУНП в Дніпропетровській області із заявою про кримінальне правопорушення, у якій просила внести відомості до ЄРДР за ст. 182 КК України ... але ВП № 3 не прийнято рішення за її заявою...»

В судовому засіданні було встановлено, що скаржницею «було повідомлено до чергової частини ВП № 3 у телефонному режимі про злочин, вчинений щодо неї ОСОБА_5, який погрожував зґвалтувати її, а також розповсюдити матеріали порнографічного характеру із зображенням її обличчя, також погрожував надсилати такі матеріали її дочці та у спільну групу на Вайбер...»

Дане повідомлення було зареєстровано поліцією, але не внесено до ЄРДР, внаслідок чого слідчий суддя зобов'язав службових осіб відділення поліції внести до ЄРДР відповідні відомості про кримінальне правопорушення.

РОЗДІЛ 6:

ДЕЯКІ ПИТАННЯ ДОКАЗІВ ТА ДОКАЗУВАННЯ

Загальні підстави здійснення досудового розслідування, закріплені в Розділі III КПК України, і їх аналіз дають підстави стверджувати, що досудове розслідування кіберзлочинів, у тому числі й тих, які містять ознаки ГЗН, чинним законодавством здійснюється на загальних умовах.

Чинним законодавством окремо визначені повноваження слідчих (дізнавачів) та оперативних підрозділів, до яких віднесено і **Департамент кіберполіції**, створений на виконання Постанови Кабінету Міністрів України від 13.10.2015 №831 «Про утворення територіального органу Національної поліції»³⁸ як міжрегіональний територіальний орган Національної поліції (далі – Департамент кіберполіції), який відповідно до законодавства України здійснює оперативно-розшукову діяльність.

Отже, повноваження працівників органу досудового розслідування визначені ст.ст. 39-40-1 КПК України, а повноваження оперативних підрозділів визначаються ст. 41 КПК України, яка чітко визначає, що оперативні підрозділи виконують надані їм доручення і не мають права здійснювати процесуальні дії у кримінальному провадженні за власною ініціативою.

При цьому під час доказування кіберзлочинів є ряд особливостей, пов'язаних з відшукуванням, фіксуванням, вилученням та збиранням таких доказів в електронній формі. Наприклад, у КПК визначено порядок:

- тимчасового доступу до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення (ст. 159);
- тимчасового вилучення електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, що здійснюється лише у разі, якщо вони безпосередньо зазначені в ухвалі суду. (ст. 168);
- втручання у приватне спілкування, зокрема, шляхом зняття інформації з електронних комунікаційних мереж та зняття інформації з електронних інформаційних систем (ст. 258, 263, 264);

38 <https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text>

- установлення місцеперебування радіообладнання (радіоелектронного засобу) (ст. 268) тощо.

Тобто, уповноважена на здійснення досудового розслідування особа може надавати доручення на здійснення тих чи інших дій фахівцям департаменту кіберполіції з подальшим включенням результатів виконання доручень до матеріалів досудового розслідування, наприклад:

Обґрунтовуючи необхідність накладення арешту на майно в рамках кримінального провадження, прокурор у своєму клопотанні зазначив:

«В ході виконання доручення слідчого, працівниками ВПК в Київській області Департаменту кіберполіції Національної поліції України встановлено, що працівники офісного приміщення, розташованого в квартирі АДРЕСА_1, займаються адмініструванням акаунтів моделей жіночої статі на платформі "OnlyFans" та веб-ресурсах для онлайн спілкування та знайомств за допомогою веб-камери "ІНФОРМАЦІЯ_1", "ІНФОРМАЦІЯ_2" та "ІНФОРМАЦІЯ_3", "ІНФОРМАЦІЯ_4". Із використанням вказаних веб-ресурсів, працівники вказаного офісу займаються виготовленням, зберіганням, збутом та розповсюдження предметів порнографічного характеру з громадянами різних країн через Інтернет мережу. ...

В ході слідства працівниками ВПК в Київській області Департаменту кіберполіції Національної поліції України проведено огляди вищевказаної вилученої техніки та на якій зафіксовано значний масив матеріалів порнографічного характеру....»

*Ухвала слідчого судді Печерського районного суду м. Києва від
05.01.2024 у справі №757/285/24-к*

Обґрунтовуючи необхідність застосування запобіжного заходу у вигляді тримання під вартою, слідчий у своєму клопотанні зазначив «про достатність даних, які вказують на причетність підозрюваного до вчинення інкримінованого йому діяння, що підтверджується доданими до клопотання матеріалами, а саме:... -матеріалами виконаного доручення Департаментом кіберполіції управління протидії кіберзлочинам в місті Києві, якими встановлено та оглянуто відеозаписи на веб-ресурсах каналу у соціальній мережі (месенджері) "Telegram" з назвою "ІНФОРМАЦІЯ_2" ..."

*Ухвала слідчого судді Шевченківського районного суду м. Києва від
03.02.2023 у справі №761/4127/23*

Обґрунтовуючи необхідність проведення обшуку, слідчий у своєму клопотанні зазначив:

«У ході проведення досудового розслідування слідчим у кримінальному провадженні було надано доручення працівникам оперативного підрозділу Кіберполіції НП України з метою проведення огляду веб-ресурсів, на яких здійснюється створення кіно - та відеопродукції, інших предметів порнографічного характеру.

Так, працівниками Кіберполіції НП України 26.03.2020 було проведено огляд веб-ресурсу із ім'ям "www.camwhores.tv", в ході якого було виявлено відео файл із назвою "SecretPearl free webcam show 2018-09-07_223424".»

*Ухвала слідчого судді Святошинського районного суду м. Києва від
14.05.2020 у справі №759/7640/20*

РОЗДІЛ 7:

ПОВНОВАЖЕННЯ КІБЕРПОЛІЦІЇ

У ході підготовки цього аналізу виникла необхідність в отриманні інформації про обсяг повноважень Департаменту кіберполіції та деяких статистичних даних.

Враховуючи, що у відкритому доступі відсутня інформація про обсяг повноважень Департаменту кіберполіції, інформація про обсяг повноважень даного підрозділу була отримана з відповіді на запит.³⁹

Так, Департамент кіберполіції забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, захист прав та свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із протидії кіберзлочинам, підвищення поінформованості громадян про безпеку в кіберпросторі. Одним із його завдань є участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Відповідно до покладених на Департамент кіберполіції завдань та положень Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події⁴⁰ він не є слідчим підрозділом та не має повноважень на внесення повідомлень про кримінальні правопорушення до ЄРДР.

У вищевказаній відповіді на запит Департамент кіберполіції зазначає, що на його адресу протягом 2022 року надійшло 70 тис. звернень громадян, а у 2023 році 78.5 тис. звернень, але "ведення статистики щодо тематики звернень та віку заявників, не передбачено".

Отже, Департамент кіберполіції виконує оперативно-розшукову діяльність і, відповідно до його офіційної статистики, яка публікується в загальному доступі, можна побачити обсяг здійсненої роботи, наприклад:

За результатами роботи у 2022 році:

«У 2022 році кіберполіцейськими здійснювалось супроводження 5 тис. кримінальних правопорушень, виявлено 2,3 тис. кіберзлочинів, повідомлено про підозру 1 тис. особам за вчинення 2,3 тис. кримінальних правопорушень. Затримано понад 100 кіберзлочинців, задокументо-

39 https://drive.google.com/file/d/107fARvxvMoZkO7GOYTXtiQU_Y4Wd-eB7/view?usp=sharing

40 <https://zakon.rada.gov.ua/laws/show/z0223-19#Text>

вано та притягнуто до відповідальності 30 педофілів та 10 хакерів. До суду з обвинувальними актами скеровано 2,7 тис. кримінальних правопорушень за обвинуваченням 840 осіб»⁴¹.

за результатами роботи у 2023 році:

«Виявлено понад 3600 кіберзлочинів

За оперативного супроводу кіберполіції оголошено підозру понад 1700 особам за вчинення понад 3700 злочинів, що на 59% перевищує аналогічний показник у 2022 році

Направлено до суду матеріали щодо 42 організованих злочинних груп, у тому числі 7 злочинних організацій, що на 83% перевищує аналогічний показник у 2022 році»⁴².

При цьому окремої статистики за кількістю ГЗК у зазначені періоди Департаментом кіберполіції не велося.

Для отримання статистичних даних по ГЗК до Офісу Генерального прокурора, як до власника і розпорядника ЄРДР, було подано запит з проханням надати інформацію про кількість одержаних та внесених до ЄРДР звернень/заяв повнолітніх жінок (їх законних представників чи представниць) та неповнолітніх дівчат віком від 14 років (їх законних представників чи представниць) про вчинення стосовно них кіберзлочинів, пов'язаних з переслідуванням у мережі Інтернет, погрозою застосування фізичного насильства, порушенням недоторканності приватного життя, розповсюдженням персональних даних, у тому числі фото/відео різного змісту, а також звернень/заяв/справ з указаних питань, що надійшли від органів Національної поліції (по кожному злочину окремо) та результатів їх досудового розслідування.

Інформація, отримана на даний запит, свідчить про відсутність статистики, оскільки Офіс Генерального прокурора повідомив, що «звітності, яка формується органами прокуратури, не передбачено облік даних за запитуваними параметрами. Крім того, згідно з даними інформаційної системи "Система електронного документообігу органів прокуратури України" упродовж 2022-2023 років в Офісі Генерального прокурора зареєстровано майже 519 тис. вхідних документів з яких, ураховуючи особливості формування реєстра-

41 <https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczni-969/>

42 <https://www.facebook.com/watch/?v=722135096772255>

ційно-моніторингових карток та відсутність посилання на конкретні дані, виокремити документи із зазначених у запиті питань неможливо».

Як зазначалося вище, більша частина кримінальних правопорушень, які можна охарактеризувати як кіберзлочини, міститься в КК України у Розділі XVI. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Аналіз статистичної звітності, оприлюдненої на офіційному сайті Офісу Генерального прокурора, показує, що інформація про ГЗК окремо не обліковується, але статистика саме по цьому розділу Кримінального кодексу України ведеться і стосовно даної інформації:

- за три квартали 2024 року обліковано кримінальних правопорушень - 3420, направлено до суду з обвинувальним актом - 2005;
- за 2023 рік обліковано кримінальних правопорушень - 3667, направлено до суду з обвинувальним актом - 2401;
- за 2022 рік обліковано кримінальних правопорушень - 3279, направлено до суду з обвинувальним актом - 2426.

Отримана інформація показує зростання кіберзлочинів загалом, навіть без прив'язки до кримінальних правопорушень, які містять ознаки ГЗН.

РОЗДІЛ 8:

ДОСЛІДЖЕННЯ СУДОВИХ РІШЕНЬ

Враховуючи, що Департамент кіберполіції, як спеціалізований структурний підрозділ Національної поліції України, працює в складі кримінальної поліції та здійснює оперативно-розшукову діяльність, а також відсутність офіційної статистики стосовно ГЗК, було прийнято рішення дослідити питання залученості працівників департаменту до кримінальних проваджень через моніторинг судових рішень судів першої інстанції за період 2023 року та першого півріччя 2024 року.

Дослідження судових рішень базувалося на використанні відкритих судових реєстрів, зокрема ЄДРСР⁴³ – автоматизованої системи збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень, до якої, відповідно до Закону України «Про доступ до судових рішень»⁴⁴ та Порядку ведення Єдиного державного реєстру судових рішень⁴⁵, судами вносяться всі тексти судових рішень, викладені в письмовій формі.

Для проведення моніторингу з метою оптимізації обсягу інформації, яка аналізується, пошук було здійснено за такими індикаторами:

Варіант 1:

- графа “пошук за контекстом” – внесено кіберп* OR кіберб*⁴⁶;
- графа “період ухвалення (постановлення)” – зазначено відповідний період;
- графа “форма рішення” – зазначено “вирок” та “ухвала”;
- графа “форма судочинства” – зазначено “кримінальне”;
- графа “категорія справ” – зазначено “кримінальні справи з 01.01.2019”;
- в графах підкатегорій зазначалися відповідні розділи Особливої частини КК України.

За вказаними індикаторами було отримано та проаналізовано 371 судове рішення, яке містило в тексті згадування індикаторів “кіберп” або “кіберб”. Отримана інформація була зведена за відповідними розділами Особливої частини КК України й наочно ілюструє, у яких справах фахівці Департаменту кібербезпеки залучалися частіше за все.

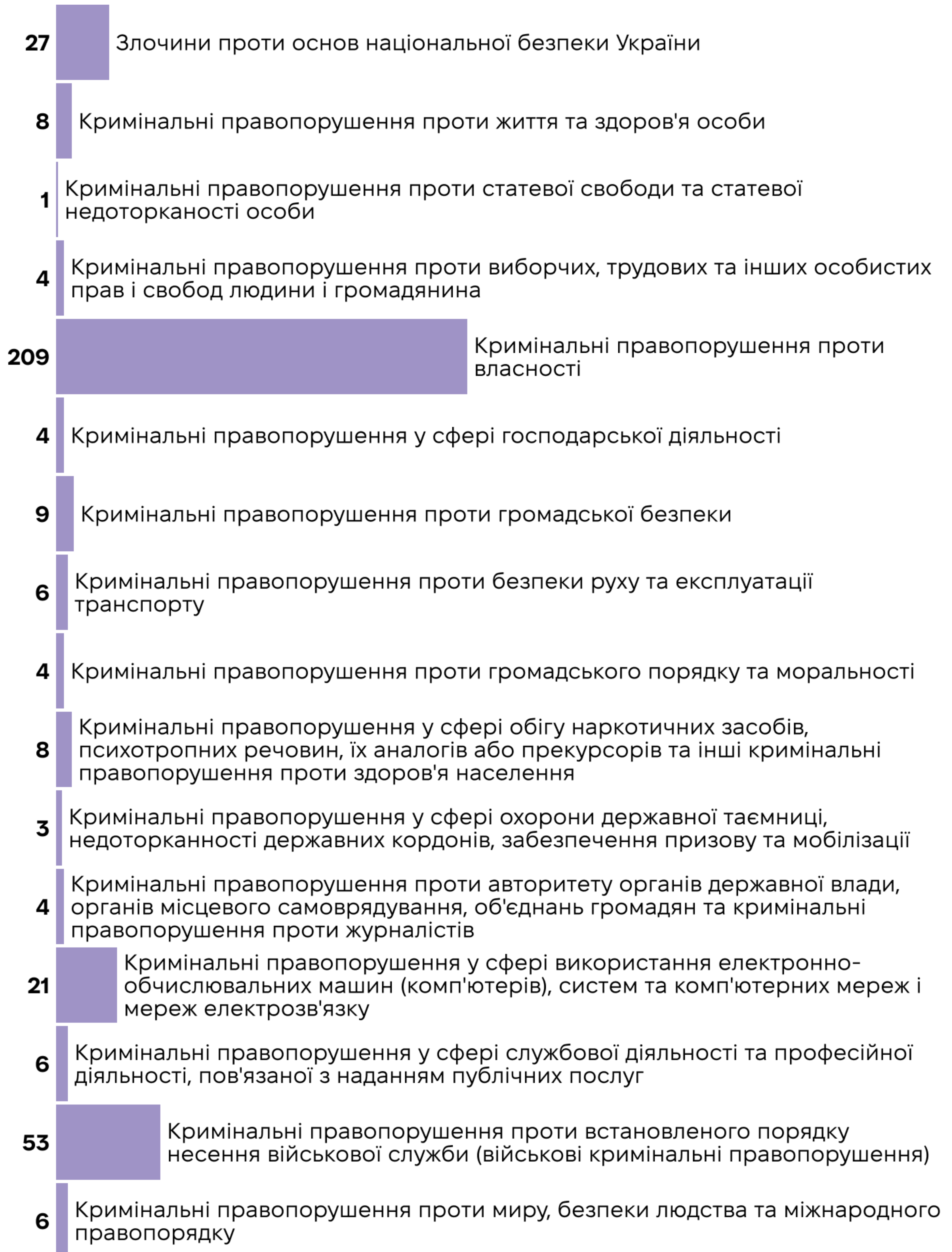
43 <https://reyestr.court.gov.ua/>

44 <https://zakon.rada.gov.ua/laws/show/3262-15#Text>

45 <https://zakon.rada.gov.ua/rada/show/v1200910-18#n1275>

46 Використовувалися скорочення від визначень “кіберполіція” та “кібербезпека”, які дали можливість більш широкого охоплення масиву судових рішень з виключенням помилок при написанні слів.

КІЛЬКІСТЬ ВИОКРЕМЛЕНИХ СУДОВИХ РІШЕНЬ ЗА 2023 РІК ТА ПЕРШЕ ПІВРІЧЧЯ 2024 РОКУ



РОЗДІЛ 9:

РОЗВИТОК МІЖНАРОДНОГО ЗАКОНОДАВСТВА

З одного боку, розвиток інтернет-технологій та соціальних мереж стирає кордони у спілкуванні, а з іншого боку, дає можливість використання забороненого контенту та/або вчинення кіберзлочинів, в тому числі пов'язаних із ГЗН.

Питання запобігання та ефективного реагування на кіберзлочини актуальне не тільки для України, а й для будь-яких країн світу, які впроваджують реформи законодавства, що стосуються кібербезпеки, ґрунтуються на наявних інструментах і представляють нові ініціативи для подальшого поліпшення кіберстійкості.

При цьому впровадження тієї чи іншої законодавчої ініціативи не зупиняє розвиток та трансформацію законодавства.

Для прикладу, у 2017 році в Німеччині було прийнято Закон про захист прав користувачів у соціальних мережах (NetzDG), спрямований на більш ефективну боротьбу зі злочинами на ґрунті ненависті, кримінальними фейковими новинами та іншим кримінальним контентом на платформах соціальних мереж. Цей закон був відповіддю на поширення злочинів на ґрунті ненависті та іншого кримінального контенту, особливо в соціальних мережах, таких як Facebook, YouTube і Twitter (пізніше X) і покладав на провайдерів соціальних мереж низку зобов'язань.

Проте у 2024 році більшість частин цього закону було скасовано у зв'язку з прийняттям Закону про цифрові послуги, положення якого спрямовані на створення більш безпечного та відповідального онлайн-середовища.

Саме положення **Закону про цифрові послуги** є єдиним загальним набором правил для всього ЄС, які ефективніше захищають користувачів і пропонують компаніям юридичну визначеність на всьому внутрішньому ринку.

Загалом, законодавство ЄС і країн Європи рухається в напрямку розширення правових механізмів для захисту жертв ГЗН у кіберпросторі та уніфікації підходів боротьби з кіберзлочинами, які завдають шкоди жінкам і представникам уразливих груп.

ВИСНОВКИ

У сучасному світі кіберпростір став невіддільною частиною нашого життя, але водночас він перетворився на нове середовище для поширення ГЗН.

Боротьба з ГЗК вимагає скоординованих зусиль держави, громадянського суспільства та міжнародної спільноти. Лише через комплексний підхід, який поєднує законодавчі зміни, позитивний міжнародний досвід, освітні заходи та підтримку потерпілих, можливо досягти реальних змін і забезпечити захист користувачів у цифровому середовищі для всіх громадян України.

Аналіз, проведений у цьому звіті, виявив низку аспектів, які потребують негайної уваги та вжиття відповідних заходів:

1. Зростання кількості ГЗК: Розвиток цифрових технологій сприяв появі нових форм насильства, що особливо впливає на жінок і дівчат. Відсутність оперативного адаптування законодавства до цих викликів створює серйозні прогалини у захисті потерпілих та притягненні винних до відповідальності.

2. Недостатнє законодавче регулювання: Хоча деякі аспекти кібернасильства в Україні врегульовано, правова база залишається неповною. Відсутність чітких визначень і механізмів протидії ускладнює роботу правоохоронних органів і судової системи, що призводить до нерівномірного та неефективного застосування законів.

3. Потреба в міжнародній співпраці та врахуванні міжнародного досвіду: Ратифікація Стамбульської конвенції та інші міжнародні зобов'язання України вимагають інтеграції найкращих світових практик у національне законодавство та практику.

4. Відсутність статистичних даних та моніторингу: Нестача офіційної статистики щодо ГЗК ускладнює оцінку масштабів проблеми та ефективність заходів протидії.

5. Необхідність підвищення обізнаності суспільства: Багато випадків кібернасильства залишаються непоміченими або про них не повідомляють через страх, стигматизацію або недовіру до правоохоронних органів. Підвищення рівня поінформованості населення є важливим кроком для запобігання насильству та підтримки потерпілих.

РЕКОМЕНДАЦІЇ

1. РОЗРОБКА ТА ВПРОВАДЖЕННЯ СПЕЦІАЛЬНОГО ЗАКОНОДАВСТВА

Необхідно розробити спеціальне законодавство, яке б передбачало окремі статті в Кримінальному кодексі України для визначення відповідальності за різні форми кібернасильства, зокрема гендерно зумовлені.

2. ПОКРАЩЕННЯ РОБОТИ ПРАВООХОРОННИХ ОРГАНІВ

Забезпечення належної підготовки та ресурсів для поліції та судових органів у сфері розслідування та переслідування кіберзлочинів.

3. СТВОРЕННЯ СИСТЕМИ МОНІТОРИНГУ ТА ЗБОРУ ДАНИХ

Ведення обліку та аналізу статистичних даних щодо кіберзлочинів, що дозволить ефективніше реагувати на виклики та планувати заходи протидії.

4. ПІДВИЩЕННЯ ОБІЗНАНОСТІ ТА ОСВІТИ

Проведення інформаційних кампаній, семінарів та тренінгів для громадськості щодо ризиків кібернасильства, способів захисту та відповідальності за кібернасильства.

5. ПІДТРИМКА ПОТЕРПІЛИХ

Створення центрів допомоги та гарячих ліній для постраждалих від кібернасильства, де вони можуть отримати юридичну, психологічну та соціальну підтримку.

6. МІЖНАРОДНА СПІВПРАЦЯ

Активне залучення до міжнародних програм та ініціатив, обмін досвідом з іншими країнами у сфері боротьби з кібернасильством.

