



Аналітичний звіт:

“Директива ЄС 2024/1385:

Виклики та можливості для

України”



Проект фінансується
Європейським Союзом

Дослідження проведене Центр "Жіночі перспективи" в рамках ініціативи «Директива ЄС 2024/1385: виклики та можливості для України» проекту «Підтримка діяльності Української національної платформи Форуму громадянського суспільства Східного Партнерства у 2025-2026 р.», який реалізує ІЕД / ІЕР за фінансової підтримки Європейського Союзу. Зміст цієї публікації є виключною відповідальністю ГО «Центр «Жіночі перспективи» і не обов'язково відображає точку зору Європейського Союзу чи Інституту економічних досліджень та політичних консультацій.

ГО Центр “Жіночі перспективи” більш ніж 25 років працює у сфері захисту прав жінок постраждалих від гендернозумовленого насильства.

Дослідження присвячене порівняльному правовому аналізу чинних українських нормативно-правових актів з положеннями **Директиви (ЄС) 2024/1385 Європейського парламенту та Ради ЄС про протидію насильству щодо жінок та домашньому насильству** з метою виявлення прогалин та невідповідностей у національному законодавстві.

Основною метою дослідження є комплексна оцінка рівня гармонізації українського законодавства з європейськими стандартами у сфері протидії гендернозумовленому та домашньому насильству, а також формулювання конкретних рекомендацій щодо необхідних законодавчих змін для забезпечення повної відповідності вимогам ЄС.

Методологічною основою роботи є порівняльний правовий аналіз, що дозволяє системно дослідити різні аспекти правового регулювання та виявити як позитивні сторони українського законодавства, так і сфери, що потребують удосконалення відповідно до стандартів Директиви (ЄС) 2024/1385.

Результати дослідження мають практичне значення для подальшого процесу євроінтеграції України та можуть бути використані при розробці змін до чинного законодавства у сфері протидії насильству.

Вступ

Актуальність дослідження у контексті євроінтеграції України

Питання гармонізації українського законодавства з європейськими стандартами набуло особливої актуальності після отримання Україною статусу кандидата в члени ЄС у червні 2022 року. Після отримання статусу кандидата в члени ЄС у червні 2022 року Україна повинна привести своє законодавство у відповідність з європейськими стандартами.

Директива охоплює не лише традиційні форми насильства, але й нові виклики цифрової епохи, зокрема кібернасильство, що становить зростаючу загрозу для жінок у всьому світі. Враховуючи високі темпи цифровізації в Україні та поширення інтернет-технологій, адаптація національного законодавства до цих нових стандартів є критично важливою.

Мета та завдання дослідження

Мета дослідження: здійснити комплексний порівняльний аналіз законодавства України з положеннями Директиви для визначення рівня відповідності та виявлення пріоритетних напрямів гармонізації.

Основні завдання:

проаналізувати правові норми законодавства України у сфері насильства щодо жінок і домашнього насильства

ідентифікувати прогалини в регулюванні кібернасильства та цифрових форм дискримінації
оцінити механізми захисту прав постраждалих осіб та їх відповідність європейським стандартам

визначити сильні сторони українського підходу та сфери, що потребують реформування

сформулювати конкретні рекомендації щодо приведення законодавства України у відповідність з Директивою

Методологія дослідження

У дослідженні застосовано порівняльно-правовий метод у поєднанні із системним аналізом нормативно-правових актів. Основою для порівняння слугують ключові українські нормативні акти:

Кодекс України про адміністративні правопорушення

Кримінальний кодекс України (надалі - ККУ)

Кримінально процесуальний кодекс України (надалі - КПКУ)

Закон “Про забезпечення рівних прав та можливостей жінок і чоловіків”

Закон “Про запобігання та протидію домашньому насильству” та

Закон “Про засади запобігання та протидії дискримінації в Україні”.

ВИСНОВКИ

Українське законодавство у сфері протидії насильству щодо жінок та домашньому насильству містить як норми, що відповідають європейським стандартам, так і значні прогалини у їх імплементації.

Правова основа для протидії гендерно обумовленому та домашньому насильству включає механізми захисту постраждалих, процедури застосування обмежувальних заходів та систему притягнення кривдників до відповідальності, що загалом узгоджуються з міжнародними стандартами.

Критичною проблемою є відсутність правового регулювання кібернасильства. Законодавство не передбачає кримінальної відповідальності за чотири основні форми кібернасильства, що створює серйозні загрози для захисту прав постраждалих жінок

Необхідно терміново доповнити ККУ нормами про кібернасильство та забезпечити готовність правоохоронних органів і судів до розслідування та розгляду таких справ, використовуючи досвід європейських держав..

РЕКОМЕНДАЦІЇ

1. **Змінити статтю 1 Закону України "Про забезпечення рівних прав та можливостей жінок і чоловіків"** та замінити термін "насильство за ознакою статі" терміном **"гендернозумовлене насильство"**, та доповнити статтю терміном "насильство щодо жінок" - порушення прав людини й форма дискримінації стосовно жінок та означає всі акти насильства стосовно жінок за гендерною ознакою, результатом яких є або може бути фізична, сексуальна, психологічна або економічна шкода чи страждання стосовно жінок, у тому числі погрози таких дій, примус або свавільне позбавлення волі, незалежно від того, чи відбувається це в публічному або приватному житті. Це забезпечить відображення структурного характеру цього явища як прояву патріархальних відносин та того, що насильство щодо жінок є постійним проявом структурної дискримінації щодо жінок, що є наслідком історично нерівного співвідношення сил між жінками та чоловіками.

2. **Внести поняття "інтерсекційна дискримінація"** до Закону України "Про засади запобігання та протидії дискримінації в Україні" для забезпечення правового інструментарію захисту найбільш вразливих груп жінок, які зазнають множинної дискримінації за кількома ознаками одночасно, а саме расою, кольором шкіри, етнічним або соціальним походженням, генетичними особливостями, мовою, релігією чи вірою, політичними чи будь-якими іншими переконаннями, належністю до національної меншини, майновим станом, народженням, інвалідністю, віком, сексуальною орієнтацією та будь-якою іншою ознакою.

3. Доповнити ККУ новими статтями, які створюють правову основу для протидії сучасним формам кібернасильства: поширення інтимних або зманіпульованих матеріалів без згоди, кібер переслідування, кібер домагання та кібер підбурювання до насильства чи ненависті, та погрози вчинення цих дій відповідно до вимог Директиви.

Поширення інтимних або зманіпульованих матеріалів без згоди –

(а) оприлюднення за допомогою інформаційно-комунікаційних технологій (надалі - ІКТ) зображень, відео чи подібного матеріалу, що зображує відверті дії сексуального характеру або інтимні частини тіла особи, без згоди цієї особи, якщо такі дії можуть завдати серйозної шкоди цій особі;

(b) виробництво, обробка, внесення змін та подальше оприлюднення за допомогою ІКТ зображень, відео чи подібного матеріалу, що створює враження, ніби особа бере участь у відверто сексуальних діях, без згоди цієї особи, якщо такі дії можуть завдати серйозної шкоди цій особі;

Кібер-переслідування - навмисні дії з неодноразового або постійного спостереження за допомогою ІКТ за особою без її згоди або без законного дозволу на це з метою відстеження або моніторингу пересування та діяльності цієї особи, якщо такі дії ймовірно завдають тяжкої шкоди цій особі.

Кібер-домагання - (а) неодноразова або постійна участь у загрозливих діях за допомогою ІКТ, спрямованих на особу, принаймні, якщо такі дії включають погрози вчинення кримінальних правопорушень, коли ці дії можуть викликати у цієї особи серйозні побоювання за власну безпеку або безпеку її утриманців;

(b) вчинення спільно з іншими особами за допомогою ІКТ публічно доступних погрозливих або образливих дій, спрямованих на особу, якщо така поведінка може спричинити серйозну психологічну шкоду цій особі;

(c) несанкціоноване надсилання за допомогою ІКТ зображення, відео чи іншого подібного матеріалу із зображенням геніталій особи, якщо така поведінка може спричинити серйозну психологічну шкоду цій особі;

(d) оприлюднення за допомогою ІКТ матеріалів, що містять персональні дані особи, без згоди цієї особи з метою спонукання інших осіб завдати цій особі фізичної чи серйозної психологічної шкоди.

Кібер-підбурювання до насильства чи ненависті - навмисне підбурювання до насильства або ненависті, спрямоване проти групи осіб або члена такої групи за ознакою статі шляхом публічного розповсюдження за допомогою ІКТ матеріалів, що містять таке підбурювання.

4. Внести у законодавство України поняття “переслідування” - умисну поведінку, яка полягає в повторному здійсненні загрозливої поведінки, спрямованої на іншу особу, що

змушує його чи її боятися за свою безпеку, об'єднавши “звичайне” та “кібер-переслідування” в одне поняття, передбачивши його у Законі України “Про забезпечення рівних прав та можливостей жінок і чоловіків”.

5. **Визначити “переслідування” самостійним злочином** шляхом запровадження окремої статті до ККУ - забезпечивши комплексний правовий захист постраждалих осіб незалежно від того, чи мали вони будь-які стосунки з переслідувачем.

6. **Доповнити статтю 67 ККУ** (обставини, що обтяжують покарання) спеціальними пунктами, які враховують всі вимоги статті 11 Директиви, або врахувати їх у складах нових злочинів відповідно до цієї Директиви (детальніше див. Додаток В).

7. **Доповнити ККУ окремою статтею каліцтво жіночих статевих органів** (жіноче обрізання) - (а) вирізання, інфібуляція або будь-яке інше калічення всієї або будь-якої частини великих, малих статевих губ або клітора; (б) примушування або спонукання жінки чи дівчини до виконання будь-яких дій, зазначених у пункті (а). Передбачити склад цього злочину в переліку норми частини 6 статті 49 ККУ, яка встановлює спеціальне правило обчислення давності для окремих злочинів щодо малолітньої чи неповнолітньої особи.

8. **Внести зміни до КПКУ щодо впровадження онлайн-процедур подання заяв про кіберзлочини.** Це дозволить постраждалим швидко та безпечно звертатися за допомогою, не виходячи з дому, що особливо важливо у випадках кібер-переслідування.

9. Для забезпечення доступності допомоги необхідно створити **національну платформу для звернень постраждалих від кібернасильства**, яка працюватиме цілодобово та забезпечуватиме анонімність звернень. Платформа повинна мати зручний інтерфейс, підтримувати декілька мов та надавати можливість завантаження доказів онлайн.

10. Окремо доцільно розробити **мобільний додаток екстреної допомоги**, який дозволить швидко звернутися за підтримкою у критичних ситуаціях. Додаток повинен мати функцію швидкого виклику допомоги, можливість надсилання попередньо підготовлених повідомлень довіреним особам та доступ до ресурсів психологічної підтримки.

11. **Запровадити процедури швидкого видалення шкідливого контенту** протягом 24-48 годин після надходження скарги. Це потребує створення спеціального механізму взаємодії між правоохоронними органами та інтернет-провайдерами, який забезпечить баланс між захистом постраждалих та дотриманням принципів свободи слова.

12. **Створити спеціалізовані слідчі групи для боротьби з кібернасильством** у структурі Національної поліції України, які матимуть відповідну підготовку та технічне оснащення для розслідування справ про цифрове насильство. Ці підрозділи повинні працювати за єдиними методиками та стандартами, розробленими з урахуванням міжнародного досвіду.

13. **Запровадити обов'язкове навчання суддів** з питань гендернозумовленого кібернасильства про його специфіку та його вплив на постраждалих. Програма навчання повинна включати як правові аспекти, так і психологічні особливості наслідків кіберзлочинів для потерпілих.

14. **Розробити детальні методичні рекомендації** для правоохоронних органів щодо розслідування кіберзлочинів, збирання та фіксації цифрових доказів, роботи з постраждалими та свідками. Ці рекомендації мають враховувати специфіку різних типів кібернасильства та містити практичні інструкції для слідчих.

1. Загальні положення

Директива була прийнята 14 травня 2024 року і стала важливим кроком у боротьбі з насильством щодо жінок та домашнім насильством у всіх країнах Європейського Союзу. Цей документ встановлює спільні мінімальні стандарти, які мають імплементувати всі держави-члени ЄС до 6 червня 2027 року.

Основна мета документа полягає у створенні комплексної системи захисту від традиційних та нових форм насильства, особливо тих, що відбуваються у кіберпросторі.

Директива визнає **насильство щодо жінок постійним проявом структурної дискримінації та серйозним порушенням основних прав людини**, а також наголошує, що її слід впроваджувати з урахуванням гендерно чутливої позиції.

При цьому слід зазначити, що попри широке використання терміну **“насильство щодо жінок”** в міжнародному праві та, зокрема, у ратифікованій Україною Стамбульській конвенції, **в національному законодавстві воно не має окремого законодавчого визначення.**

Натомість вживається термін “насильство за ознакою статі” як “діяння, спрямовані проти осіб через їхню стать, або поширені в суспільстві звичаї чи традиції (стереотипні уявлення про соціальні функції (становище, обов'язки тощо) жінок і чоловіків), або діяння, що стосуються переважно осіб певної статі чи зачіпають їх непропорційно, які завдають фізичної, сексуальної, психологічної або економічної шкоди чи страждань, включаючи погрози таких дій, у публічному або приватному житті” (стаття 1 Закону України “Про забезпечення рівних прав та можливостей жінок і чоловіків”).

Стаття 173-6 “Вчинення насильства за ознакою статі” Кодексу України про адміністративні правопорушення визначає “насильство за ознакою статі” як “умисне вчинення будь-яких діянь (дій або бездіяльності) фізичного, психологічного чи економічного характеру, спрямованих проти конкретної особи через її належність до певної статі чи стереотипні уявлення про соціальні ролі (становище, обов'язки, поведінку тощо) жінки або чоловіка в суспільстві, внаслідок чого була завдана шкода фізичному (без спричинення тілесних ушкоджень) або психічному здоров'ю потерпілого”.

ККУ демонструє повну відсутність гендерноорієнтованого підходу до насильства. Жодна стаття не містить прямої криміналізації гендернозумовленого насильства або спеціальних кваліфікуючих ознак, що враховували б гендерні мотиви. Навіть стаття 126-1 “Домашнє насильство”, попри те що жінки становлять більшість потерпілих, і домашнє насильство щодо жінок має гендернозумовлену природу, залишається гендерно нейтральною у формулюванні.

Така ситуація унеможливорює адекватну правову оцінку злочинів, мотивованих намірами підпорядкувати, принизити або контролювати жінок через їхню гендерну приналежність.

Правоохоронні органи та суди позбавлені необхідних інструментів для кваліфікації та розслідування злочинів з урахуванням їх гендерної специфіки.

Термін “наси́льство за ознакою статі” був штучно внесений до законодавства, не зважаючи на те, що визначення терміну у законі передає суть саме гендернозумовленого насильства. Термін “наси́льство за ознакою статі” не відображає історичний та структурний характер насильства щодо жінок як результату патріархальних відносин. І як наслідок, є недостатнім не лише для повноцінного виконання Україною своїх міжнародних зобов'язань, а й для створення ефективної системи захисту жінок, як вразливої групи, розробки адекватних політик протидії гендернозумовленому насильству та забезпечення фокусу на реальних масштабах та специфіці проблеми.

Директива звертає увагу на те, що насильство щодо жінок і домашнє насильство може загостритися, якщо воно перетинається з дискримінацією за ознакою статі та будь-якою іншою ознакою чи ознаками дискримінації, а саме расою, кольором шкіри, етнічним або соціальним походженням, генетичними особливостями, мовою, релігією чи вірою, політичними чи будь-якими іншими переконаннями, належністю до національної меншини, майновим станом, народженням, інвалідністю, віком чи сексуальною орієнтацією («інтерсекційна дискримінація»).

Тому **Директива закликає приділяти належну увагу постраждалим від інтерсекційної дискримінації**, вживаючи конкретних заходів, особливо щодо індивідуальної оцінки для визначення потреб постраждалих у захисті, спеціалізованої підтримки постраждалих та навчання фахівців, які можуть вступити в контакт з постраждалими.

Відсутність у національному законодавстві поняття "інтерсекційна дискримінація" створює додаткові перешкоди для захисту найбільш вразливих груп жінок, які зазнають множинної дискримінації за кількома ознаками одночасно. Жінки з інвалідністю, жінки етнічних меншин, літні жінки та жінки з ЛБТІ+ спільноти, зокрема, потребують спеціалізованих підходів, які неможливо розробити без відповідного правового інструментарію.

Директива поєднує кримінально-правові норми з нормами про права постраждалих осіб, превентивні заходи та міжнародну співпрацю, приділяючи особливу увагу цифровій безпеці.

Директива є першим актом законодавства ЄС, який **комплексно регулює кібернаси́льство проти жінок**, визнаючи, що воно диспропорційно вражає жінок. Документ встановлює чіткі критерії криміналізації, вимагаючи, щоб поведінка була здатною завдати серйозної фізичної або психологічної шкоди або викликати обґрунтовані серйозні побоювання за безпеку.

Порівняння законодавства України з Директивою показує, що попри наявність в нашій державі достатньо міцного фундаменту для боротьби з гендерно зумовленим насильством, існують критичні прогалини, які потребують негайного усунення.

Особливо гостро стоїть питання кібернасильства, де українське право значно відстає від сучасних європейських стандартів.

2. Кібернасильство: найбільш проблемна зона

Директива наголошує на необхідності “передбачити узгоджені визначення правопорушень і покарань щодо певних форм кібернасильства”, виділяючи такі ключові характеристики кібернасильства:

1) **цифрова природа** - кібернасильство "нерозривно пов'язане з використанням інформаційно-комунікаційних технологій (ІКТ)", тобто технології не є просто інструментом, вони нерозривно інтегруються у структуру злочину, змінюючи його ознаки та створюючи якісно новий тип правопорушень, відмінний від традиційного насильства;

2) **віральний характер шкоди** - використання ІКТ створює умови для легкого, швидкого та широкого розповсюдження певних форм кібернасильства з явним ризиком спричинення або посилення серйозної та тривалої шкоди постраждалій особі.

При цьому, Директива зосереджується лише на найсерйозніших формах кібернасильства, тому не кожна неприємна або образлива дія в інтернеті автоматично стає злочином. Щоб поведінка кваліфікувалася як кримінально караний злочин, вона повинна відповідати одному з двох критеріїв: **по-перше, дії мають бути здатними завдати серйозної фізичної або психологічної шкоди постраждалій, по-друге, поведінка може вважатися злочинною, якщо вона здатна викликати у постраждалої обґрунтовані серйозні побоювання за власну безпеку або безпеку її утриманців.**

Аналізований документ наголошує на тому, що кібернасильство особливо спрямоване на жінок-політикинь, журналісток і правозахисниць (під останніми розуміють осіб, групи чи організації, які просувають і захищають загальноновизнані права людини та основоположні свободи). Таке насильство може змушувати жінок мовчати та перешкоджати їхній участі в громадському житті нарівні з чоловіками. Директива також підкреслює, що кібернасильство непропорційно впливає на жінок і дівчат у навчальних закладах, таких як школи та університети, з шкідливими наслідками для їх подальшої освіти та психічного здоров'я, спричиняючи соціальну ізоляцію, занепокоєння та спонукаючи до самоушкодження та може, у крайніх випадках, довести до самогубства.

При цьому, у Директивою встановлюють лише мінімальні стандарти боротьби з кібернасильством. Це означає, що кожна країна може зробити свої закони ще суворішими, якщо вважає це необхідним для захисту своїх громадян.

Таким чином, Директива визначає кібернасильство як якісно новий тип злочинності, унікальний феномен, що потребує спеціального правового регулювання та не може бути адекватно врегульований нормами про традиційні форми насильства.

а) Проблеми застосування норм Кодексу України про адміністративні правопорушення

У 2024 році Кодекс України про адміністративні правопорушення було доповнено статтею 173-6 "Вчинення насильства за ознакою статі" та 173-7 "Сексуальне домагання". На перший погляд, ці норми могли б частково застосовуватися до окремих випадків кіберзлочинів, передбачених статтями 6, 7 та 8 Директиви ЄС 2024/1385.

Стаття 173-6 КУпАП визначає насильство за ознакою статі як умисне вчинення діянь фізичного, психологічного чи економічного характеру, спрямованих проти особи через її належність до певної статі або стереотипні уявлення про гендерні ролі. Формально, деякі прояви кібер-переслідування та кібер-домагання можуть підпадати під це визначення, адже часто такі злочини мають виражений гендерний характер і спрямовані переважно проти жінок.

Стаття 173-7 КУпАП встановлює відповідальність за сексуальне домагання, визначаючи його як умисне вчинення образливих дій сексуального характеру проти бажання особи, **у тому числі з використанням електронних комунікацій**. Це формулювання дозволяє охопити певні форми онлайн-домагання, зокрема надсилання небажаних сексуальних повідомлень або зображень через цифрові канали.

Однак детальний аналіз демонструє, що таке застосування є концептуально неправильним і не відповідає вимогам європейського законодавства.

Так, Директива ЄС 2024/1385 однозначно вимагає криміналізації кіберзлочинів, тобто визнання їх саме кримінальними правопорушеннями з відповідними санкціями. Статті 6, 7 та 8 Директиви прямо зазначають, що відповідні діяння повинні каратися "як злочин" ("shall be punishable as a criminal offence"). Це підкреслює серйозність проблеми кібернасильства, його системний характер та необхідність застосування всього арсеналу правових інструментів, доступних лише у кримінальному провадженні.

Натомість статті 173-6 та 173-7 КУпАП належать до адміністративного законодавства і передбачають виключно адміністративну відповідальність. Це принципово різні правові категорії, що мають різну суспільну оцінку, різні процедури розслідування та різні наслідки для правопорушників.

Санкції, передбачені цими адміністративними статтями, є вкрай неадекватними масштабу шкоди від кіберзлочинів і є неспівмірними з вимогами Директиви.

Процедурні аспекти також створюють непереборні бар'єри. Адміністративні правопорушення розглядаються у спрощеному порядку, часто в стислі терміни, без повноцінного розслідування та без можливості застосування спеціальних слідчих дій. Кіберзлочини ж вимагають складного технічного розслідування, збирання цифрових доказів, отримання інформації від інтернет-провайдерів, міжнародної правової допомоги. Адміністративне провадження просто не має інструментів для ефективного розслідування складних випадків кібернасильства, особливо коли злочинці використовують знеособлення, зарубіжні сервери або складні технічні схеми.

б) Проблеми застосування норм Кримінального кодексу України

Кримінальний кодекс України не містить спеціальних норм щодо кібернасильства чи окремих його форм. Щобільше, Кримінальним кодексом України прямо не криміналізовано жоден із проявів насильства над жінками - притягнення до відповідальності можливе лише із застосуванням інших норм, які не відображають гендерний характер такого насильства.

Кримінальний кодекс України демонструє повну неготовність до регулювання кібернасильства. Наявні у розділі XVI норми про "комп'ютерні злочини" зосереджуються виключно на технічних порушеннях інформаційної безпеки та не мають жодного відношення до гендерно зумовленого насильства. Стаття 361 про неправомірний доступ, стаття 361-1 про шкідливі програми та стаття 362 про несанкціоновані дії з інформацією, не охоплюють жодної з форм кібернасильства, визначених Директивою.

Одночасно, частина сучасних форм кібернасильства охоплюється нормами, які були створені до масового розвитку інтернету для криміналізації традиційних форм правопорушень, однак можуть застосовуватися незалежно від способу їх вчинення, тобто в тому числі з використанням ІКТ.

Однак, існуючі норми не враховують ні особливості злочинів з використанням ІКТ в цілому, ні сформульовані Директивою ключові характеристики кібернасильства, а також його гендерну природу.

Система покарань також потребує перегляду, оскільки санкції за традиційні злочини часто не відповідають масштабу можливої шкоди від кіберзлочинів.

Директива визначає кілька нових видів злочинів у цифровому просторі, які практично відсутні у вітчизняному законодавстві:

- **поширення інтимних або зманіпульованих матеріалів без згоди** (non-consensual sharing of intimate or manipulated material), стаття 5
- **кібер-переслідування** (cyber stalking), стаття 6
- **кібер-домагання** (cyber harassment), стаття 7 та
- **кібер-підбурювання до насильства чи ненависті** (cyber incitement to violence or hatred) (стаття 8).

Поширення інтимних або зманіпульованих матеріалів без згоди (non-consensual sharing of intimate or manipulated material), стаття 5

Стаття 5 вимагає криміналізації такої навмисної поведінки:

(a) оприлюднення через інформаційно-комунікаційні технології зображень, відео або подібних матеріалів, що зображують сексуально відверті дії або інтимні частини особи без згоди цієї особи, де така поведінка може спричинити серйозну шкоду цій особі;

(b) виготовлення, маніпулювання або зміна та подальше оприлюднення через ІКТ матеріалів, що створюють враження ніби особа займається сексуальною діяльністю, без згоди цієї особи;

(c) погрози здійснити таку поведінку з метою примусу особи.

Директива передбачає покарання за такі діяння у вигляді позбавлення волі, верхня межа строку якого не може бути меншою 1 року.

Кримінальне законодавство України не містить окремих статей, які покривають кожен із складів злочину, передбачені статтею 5 Директиви. Однак, певні норми ККУ дозволяють притягнути до кримінальної відповідальності за окремі прояви такої протиправної поведінки.

До прикладу для притягнення до відповідальності **за неконсенсуальне поширення інтимних матеріалів (пункт а статті 5 Директиви)** може застосовуватися стаття 182 «Порушення недоторканності приватного життя» ККУ. Вона передбачає кримінальну відповідальність за неправомірне збирання, зберігання, використання та поширення конфіденційної інформації про особу.

Основним об'єктом злочину є право людини на приватність та захист особистої інформації, а предметом — конфіденційна інформація. Зміст «конфіденційної інформації» як обов'язкової, самостійної ознаки цього злочину складає достатньо широкий спектр відомостей і даних про особисте чи сімейне життя фізичної особи (що дозволяють її ідентифікувати), стосовно яких в особи є законні очікування (через визначення режиму їх застосування) щодо нерозголошення відповідних відомостей і даних без її на те згоди. Зображення (відео чи подібні матеріали) особи інтимного характеру, у контексті застосування статті 182 КК, можуть вважатися конфіденційною інформацією про неї.

"Поширення" конфіденційної інформації охоплює надання доступу до неї будь-яким способом, у тому числі цифрове поширення через ІКТ, як це передбачено у Директиві.

"Незаконним" у статті 182 ККУ вважається поширення без згоди особи або всупереч встановленим законом обмеженням, що також відповідає нормі Директиви.

Основний склад злочину статті 182 ККУ є формальним і не залежить від здатності діяння заподіяти серйозну шкоду, тоді як Директива ЄС криміналізує неконсенсуальне поширення за наявності ризику серйозних наслідків або наміру їх заподіяти. Це означає, що

українське законодавство встановлює нижчий поріг криміналізації, що теоретично може забезпечити ширше коло захисту. Водночас стаття 182 ККУ є загальною нормою про порушення недоторканності приватного життя і не враховує специфіку неконсенсуального поширення інтимних матеріалів як форми сексуального та гендернозумовленого насильства, що передбачає пункт (а) статті 5 Директиви.

Разом із цим слід звернути увагу, що стаття 182 ККУ не відповідає вимогам Директиви щодо серйозності покарання. Адже санкція статті 182 ККУ передбачає такі альтернативні види покарання як штраф, виправні роботи, пробаційний нагляд чи обмеженням волі, тоді як Директива вимагає позбавлення волі з верхню межею строку не меншою ніж 1 рік.

Крім того, склад злочину статті 182 ККУ не враховує специфіку важливості для особи інтимної сфери, її особливу вразливість, а також тяжкість потенційної шкоди, завданої втручанням у цю сферу: психологічна травма, суїцидальні наміри, соціальна стигматизація тощо. На додаток, поза увагу залишається гендерний аспект, закладений у статті 5 Директиви: жінки диспропорційно постраждають від таких злочинів. Поза увагою залишається також той факт, що поширення конфіденційної інформації через інтернет є в рази швидшим та масштабнішим.

До випадків поширення інтимних зображень, які мають порнографічний характер може також застосовуватися стаття 301 ККУ "Ввезення, виготовлення, збут і розповсюдження порнографічних предметів". Однак, вона охороняє від розповсюдження порнографічного контенту загалом та спрямована на захист громадського порядку та суспільної моралі: а не на захист від кіберзлочинів та боротьбу з насильством щодо жінок як це передбачає Директива. Крім того, санкція статті 301 ККУ не передбачає позбавлення волі, як цього вимагає Директива.

Аналогічні недоліки має також застосування для окремих випадків поширення інтимних зображень норм статей 301-1 ККУ "Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження" та 301-2 ККУ "Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи" попри те, що їх склади прямо передбачають використанням інформаційно-телекомунікаційних систем чи технологій.

Пункт (b) статті 5 Директиви охоплює *"виробництво, обробку, внесення змін та подальше оприлюднення за допомогою ІКТ зображень, відео чи подібного матеріалу, що створює враження, ніби особа бере участь у відверто сексуальних діях, без згоди цієї особи, якщо такі дії можуть завдати серйозної шкоди цій особі"* (deepfakes).

Ключові елементи складу згідно з Директивою:

- продукування візуального контенту, що створює фальшиве враження про участь особи в сексуальних діях
- публічне поширення такого контенту за допомогою ІКТ

- відсутність згоди особи
- можливість завдання серйозної шкоди
- використання технології deepfakes та AI-маніпуляцій

Застосування статті 182 "Порушення недоторканності приватного життя" до deepfakes та AI-маніпуляцій має суттєві концептуальні недоліки.

По-перше, deepfakes не є "конфіденційною інформацією про особу" у традиційному правовому розумінні. Хоча справжні інтимні зображення особи можуть вважатися конфіденційною інформацією на підставі конституційного права на приватність, цивільно-правового регулювання права на зображення та судової практики, штучно створений контент не містить реальної інформації про особу. Deepfakes лише створюють хибне враження про її дії або поведінку, використовуючи зображення як технічну основу.

По-друге, процес створення deepfakes не підпадає під поняття "незаконна зміна конфіденційної інформації". Це не модифікація існуючих матеріалів, а генерація абсолютно нового фальшивого контенту за допомогою алгоритмів машинного навчання, що принципово відрізняється від традиційного розуміння "зміни інформації".

По-третє, стаття 182 ККУ не містить механізмів для врахування публічного характеру поширення за допомогою ІКТ як кваліфікуючої ознаки, що є ключовим елементом шкоди від deepfakes.

Якщо створені матеріали мають порнографічний характер, теоретично можливе застосування статті 301 "Ввезення, виготовлення, збут і розповсюдження порнографічних предметів" через елементи "виготовлення" та "розповсюдження порнографічних предметів". Судова практика визнає, що до порнографічних предметів належать як матеріальні носії, так і зображення, створені в режимі онлайн.

Однак застосування статті 301 ККУ до deepfakes має істотні недоліки. Ця норма була створена для боротьби з порнобізнесом та вимагає мети "збуту чи розповсюдження", тоді як виготовлення deepfakes часто має на меті приниження, шантаж або психологічне насильство проти конкретної особи.

Стаття 301 ККУ не враховує також ключову особливість deepfakes - зманіпульований характер матеріалів та відсутність реальної участі зображеної особи в сексуальних діях. Це принципово відрізняє deepfakes від традиційної порнографії.

Deepfakes та інші AI-маніпуляції мають унікальні характеристики, що принципово відрізняють їх від традиційних форм підробки або порушення приватності. Ці технології дозволяють створювати надзвичайно реалістичний контент, який може бути неможливо відрізнити від справжнього навіть для експертів.

ККУ не враховує специфічні технологічні процеси виготовлення deepfakes, які потребують використання складних алгоритмів машинного навчання, великих баз даних зображень та

значних обчислювальних ресурсів. Ця технологічна складність має правові наслідки для кваліфікації діянь та визначення суб'єктів відповідальності. Особливо проблематичним є питання відповідальності розробників AI-технологій, операторів платформ, що надають сервіси для створення deepfakes, та осіб, що надають обчислювальні потужності для таких цілей. ККУ не має норм для регулювання цих аспектів.

Deepfakes мають особливо руйнівний психологічний вплив на постраждалих порівняно з традиційними формами порушення приватності. Неможливість довести фальшивість матеріалів для широкої аудиторії, постійний ризик їх повторного поширення та довготривалий вплив на репутацію створюють унікальну форму психологічної травми. ККУ не враховує цю специфіку при визначенні ступеня суспільної небезпеки та відповідних санкцій.

Традиційними нормами про порушення приватності не враховується ґендерний контекст у регулюванні створення фальшивих інтимних зображень. Це не дозволяє врахувати специфічну шкоду, яка може завдаватися жінкам через такі технології, включаючи примушення до самоцензури та відмови від публічної активності.

Існуючі санкції за порушення приватності або поширення порнографії не відповідають серйозності та унікальності шкоди від deepfakes. Довготривалий вплив на репутацію, складність спростування фальшивих матеріалів та потенціал для повторного використання потребують значно суворіших покарань.

Пункт (с): Погрози поширенням інтимних матеріалів

Пункт (с) статті 5 Директиви криміналізує умисне поширення, передачу або надання доступу третім особам до інтимних зображень живої особи або відео з такою особою без згоди цієї особи, коли такі дії заподіюють значну шкоду гідності відповідної особи. Особливістю цього положення є також охоплення випадків використання штучного інтелекту або аналогічних технологій для створення або маніпулювання зображеннями, відео чи аудіоматеріалами, що створюють хибне враження реальності.

Аналізуючи чинні норми ККУ, найбільш релевантною видається стаття 182 "Порушення недоторканності приватного життя". Ця норма встановлює відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконне поширення такої інформації. Теоретично інтимні матеріали можуть розглядатися як різновид конфіденційної інформації про особу, що дає підстави для застосування цієї статті.

Проте практичне застосування статті 182 ККУ до випадків погроз поширенням інтимних матеріалів (revenge porn) виявляє суттєві обмеження. Формулювання норми є занадто абстрактним і не враховує специфічну природу шкоди, що завдається поширенням інтимних матеріалів. Крім того, термін "конфіденційна інформація" потребує додаткового тлумачення у контексті інтимних зображень або відео, що створює правову невизначеність.

Стаття 163 ККУ "Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції" також може розглядатися як потенційно застосовна, але її фокус на процесі перехоплення інформації, а не на її подальшому поширенні, робить її малоефективною для боротьби з неконсенсуальним поширенням інтимних матеріалів. Більше того, ця стаття історично орієнтована на традиційні форми комунікації і не враховує особливостей сучасного цифрового простору та онлайн-платформ.

Особливо проблематичною є відсутність у ККУ будь-яких норм, що стосуються використання технологій штучного інтелекту для створення зманіпульованих інтимних матеріалів. Deepfake-технології дозволяють створювати надзвичайно реалістичні, але повністю сфабриковані інтимні зображення або відео будь-якої особи. Такі матеріали можуть завдати не меншої шкоди, ніж автентичні інтимні зображення, а іноді навіть більшої, оскільки постраждала може взагалі не знати про існування таких матеріалів до їх поширення.

Адекватність санкцій, передбачених існуючими нормами, також заслуговує на критику. Максимальне покарання за статтею 182 ККУ становить три роки позбавлення волі, що видається недостатнім з огляду на серйозність психологічних, соціальних та економічних наслідків для постраждалих від неконсенсуального поширення інтимних матеріалів. Дослідження показують, що такі злочини часто призводять до тривалої психологічної травми, соціальної ізоляції, втрати роботи та навіть суїцидальних думок у постраждалих.

Процедурні аспекти розслідування таких злочинів також потребують особливої уваги. Специфіка цифрового середовища, швидкість поширення матеріалів в інтернеті, необхідність збереження цифрових доказів та врахування міжнародного характеру багатьох онлайн-платформ створюють додаткові виклики для правоохоронних органів. Існуючі процедурні норми не повністю адаптовані до цих реалій.

Аналізуючи відповідність українського законодавства пункту (с) статті 5 Директиви, можна констатувати, що хоча деякі аспекти цього положення частково охоплюються існуючими нормами ККУ, загальний рівень відповідності є недостатнім. Основними проблемами є відсутність спеціального складу злочину, неврахування специфіки цифрового середовища, відсутність норм щодо deepfake-технологій та неадекватність санкцій.

Кібер-переслідування (cyber stalking), стаття 6

Сучасне кібер-переслідування включає систематичне стеження через соціальні мережі, використання GPS-трекінгу та моніторинг цифрових платформ для залякування постраждалої особи. Ці дії часто залишаються безкарними через відсутність спеціалізованих правових норм, адаптованих до реалій інтернет-епoxy.

Стаття 6 Директиви ЄС визначає кібер-переслідування як *“навмисні дії з неодноразового або постійного спостереження за допомогою інформаційно-комунікаційних технологій за особою без її згоди або без законного дозволу на це з метою відстеження або моніторингу*

пересування та діяльності цієї особи, якщо такі дії ймовірно завдають тяжкої шкоди цій особі, каралися як злочин”.

Стаття 34 Стамбульської конвенції визначає переслідування як *умисну поведінку, що полягає в повторному здійсненні загрозливої поведінки, спрямованої на іншу особу, що змушує його чи її боятися за свою безпеку.*

Аналіз досвіду країн, що вже запровадили кримінальну відповідальність за переслідування, демонструє відсутність практики такого законодавчого розподілу переслідування на “реальне” та “кібер”. **Переважає більшість правових систем кваліфікує переслідування як уніфікований склад злочину, що не залежить від конкретних методів його реалізації - чи то у фізичному просторі, чи в цифровому середовищі.** З огляду на те, що правопорушники зазвичай застосовують змішані стратегії, поєднуючи офлайн та онлайн методи впливу, такий підхід до нормотворення є виправданим. Він забезпечує комплексне правове регулювання різноманітних форм переслідування, запобігаючи правозастосовчим колізіям.

На сьогодні законодавство України не містить ані чіткого визначення переслідування (сталкінгу), ані прямої заборони цієї форми протиправної діяльності. Існуючі норми (стаття 182 “Порушення недоторканності приватного життя”, 163 “Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер” ККУ) можуть лише частково охопити окремі прояви переслідування, але не забезпечують комплексного захисту від цього виду насильства.

“Переслідування” згадується у переліку проявів психологічного домашнього насильства у статті 1 Закону України “Про запобігання та протидію домашньому насильству”, проте за своїм змістом виходить за межі цього насильства.

Стаття 361 “Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж” ККУ може бути застосована до кіберпереслідування лише у вузькому колі випадків, коли злочинець використовує технічні методи несанкціонованого доступу до пристроїв або систем жертви, зокрема при зломі смартфона чи комп'ютера для встановлення шпигунського програмного забезпечення (stalkerware), викраденні паролів для доступу до електронної пошти та соціальних мереж, або таємній активації програм для перехоплення даних з клавіатури. Однак ця стаття залишає поза межами кримінальної відповідальності більшість випадків кіберпереслідування, включаючи ситуації коли кривдник використовує формально легальний доступ до пристроїв чи акаунтів (наприклад, паролі отримані під час спільного проживання) чи встановлює GPS-трекери на власні речі якими користується постраждала особа. Ключова проблема полягає в тому, що стаття 361 захищає роботу інформаційних систем як таких, а не права конкретної особи на приватність та безпеку, тому вона не враховує систематичний характер переслідування, мету контролю

над жертвою та психологічну шкоду, які є центральними елементами кіберпереслідування за визначенням Директиви 2024/1385.

Кібер-домагання (Cyber harassment), стаття 7

Стаття 7 Директиви ЄС 2024/1385 передбачає чотири форми кібер-домагань:

(a) неодноразова або постійна участь у загрозливих діях за допомогою ІКТ, спрямованих на особу, принаймні, якщо такі дії включають погрози вчинення кримінальних правопорушень, коли ці дії можуть викликати у цієї особи серйозні побоювання за власну безпеку або безпеку її утриманців;

(b) вчинення спільно з іншими особами за допомогою ІКТ публічно доступних погрозливих або образливих дій, спрямованих на особу, якщо така поведінка може спричинити серйозну психологічну шкоду цій особі;

(c) несанкціоноване надсилання за допомогою ІКТ зображення, відео чи іншого подібного матеріалу із зображенням геніталій (cyberflashing) особі, якщо така поведінка може спричинити серйозну психологічну шкоду цій особі;

(d) оприлюднення за допомогою ІКТ матеріалів, що містять персональні дані особи, без згоди цієї особи з метою спонукання інших осіб завдати цій особі фізичної чи серйозної психологічної шкоди (doxing).

Щодо пункту (a) - повторювані онлайн-погрози

Стаття 129 ККУ "Погроза вбивством" частково може застосовуватися до цієї форми кібер-домагання, але має значні обмеження. По-перше, вона охоплює виключно погрози вбивством, тоді як Директива передбачає більш широкий спектр погроз вчинення кримінальних правопорушень. По-друге, стаття 129 ККУ не враховує специфіку цифрового середовища та повторюваність як ключову ознаку кібер-домагання. Важливо, що українська норма не містить елементу неодноразовості, який є критично важливим для кваліфікації кібер-домагання.

Крім того, стаття 129 ККУ не передбачає посилену відповідальність за використання ІКТ як засобу вчинення злочину, який дозволяє досягти більшого масштабу залякування та тривалішого психологічного впливу на постраждалу.

Водночас обов'язковою ознакою складу злочину за статтею 129 ККУ є наявність реальних підстав побоюватися здійснення погрози, і саме цей критерій створює додаткові бар'єри для притягнення до відповідальності за онлайн-погрози, коли відсутність фізичної присутності помилково інтерпретується як відсутність реальної небезпеки. Тому на практиці правоохоронці часто не визнають цифрові погрози достатньо реальними для відкриття кримінального провадження, незважаючи на їх потенційно серйозний психологічний вплив та можливість встановлення особи й місцезнаходження постраждалої через цифрові технології.

Щодо пункту (b) - координовані групові атаки

Ця форма кібер-домагання практично не охоплена чинним ККУ. Стаття 296 "Хуліганство" не може застосовуватися до випадків агресивної поведінки он лайн, бо вона зосереджена на порушенні громадського порядку в фізичному просторі з мотивів явної неповаги до суспільства. Координовані онлайн-атаки мають інший механізм дії та мотивацію - вони спрямовані проти конкретної особи, а не проти громадського порядку загалом.

Щодо пункту (c) - cyberflashing

Пункт (c) статті 7 Директиви передбачає криміналізацію *"несанкціонованого надсилання за допомогою ІКТ зображення, відео чи іншого подібного матеріалу із зображенням геніталій особі, якщо така поведінка може спричинити серйозну психологічну шкоду цій особі"*.

Ключові елементи cyberflashing згідно з Директивою:

- надсилання зображень геніталій через ІКТ
- небажаний характер надсилання (без згоди отримувача)
- можливість завдання серйозної психологічної шкоди
- цифровий спосіб вчинення

ККУ немає адекватного регулювання cyberflashing як окремої форми цифрового сексуального домагання. Існуючі норми можуть застосовуватися лише епізодично та з концептуальними проблемами.

Якщо надіслані зображення мають порнографічний характер, теоретично можливе застосування статті 301 "Ввезення, виготовлення, збут і розповсюдження порнографічних предметів" через елемент "розповсюдження порнографічних предметів". Однак це застосування є концептуально неточним з кількох причин.

Стаття 301 ККУ вимагає мети "збуту чи розповсюдження", тоді як cyberflashing має зовсім іншу мотивацію - залякування, сексуальне домагання, демонстрацію влади або приниження постраждалої особи. Історично ця норма застосовувалася до комерційного обігу порнографічної продукції або її масового поширення, а не до кривдження конкретних осіб.

Крім того, складно довести мету "розповсюдження" у традиційному розумінні, коли зображення надсилається конкретній особі без її бажання отримувати такий контент. Мета cyberflashing полягає не в поширенні порнографічного контенту як такого, а у використанні його як інструменту психологічного тиску або сексуального домагання.

У деяких випадках cyberflashing може розглядатися як форма психологічного примушування, особливо якщо воно супроводжується вимогами або погрозами. Однак стаття 154 "Примушування до вступу в статевий зв'язок" ККУ вимагає конкретних вимог щодо вчинення або утримання від вчинення певних дій, тоді як cyberflashing часто є самоціллю - демонстрацією непристойного контенту без конкретних вимог.

Найсерйознішою проблемою є відсутність розуміння cyberflashing як специфічної форми сексуального домагання у цифровому просторі. Це явище має унікальні характеристики, що принципово відрізняють його від традиційних форм непристойної поведінки.

Cyberflashing характеризується інтимним характером нападу - зображення надсилається безпосередньо постраждалим, часто через приватні повідомлення, що створює відчуття вторгнення в особистий простір. Це кардинально відрізняється від публічного непристойного оголення, що регулюється традиційними нормами про хуліганство.

Важливою особливістю є також те, що цифрові платформи дозволяють одному правопорушнику масово переслідувати багатьох постраждалих. Технології дозволяють миттєво надіслати непристойні зображення десяткам або сотням осіб одночасно, що створює ефект масштабування шкоди.

ККУ не враховує психологічну специфіку cyberflashing. Небажане отримання зображень геніталій може спричинити серйозну психологічну травму, особливо у дітей. Це може призводити до уникнення використання цифрових платформ, самоцензури в онлайн-просторі та обмеження участі в цифровому житті суспільства.

Міжнародні дослідження показують, що переважно чоловіки вчиняють cyberflashing проти жінок, використовуючи це як форму сексуального домагання та демонстрації влади. Цей гендерний контекст не відображений у жодній з існуючих норм ККУ.

Cyberflashing може відбуватися через різні цифрові канали - соціальні мережі, месенджери, електронну пошту, навіть через технології бездротової передачі даних у громадських місцях. Кожен з цих способів має свої особливості, що потребують спеціального правового регулювання.

Проблематичним є також анонімний характер багатьох випадків cyberflashing, коли правопорушники використовують фальшиві акаунти або технології, що ускладнюють ідентифікацію. Існуючі норми ККУ не містять спеціальних механізмів для розслідування таких злочинів.

Щодо пункту (d) - doxing

Пункт (d) статті 7 Директиви передбачає протиправні дії у вигляді оприлюднення за допомогою ІКТ матеріалів, що містять персональні дані особи, без згоди цієї особи з метою спонукання інших осіб завдати цій особі фізичної чи серйозної психологічної шкоди.

Отже, елементами складу doxing згідно Директиви є:

- публічне поширення особистих даних через ІКТ
- відсутність згоди особи
- спеціальна мета - спонукання третіх осіб до завдання шкоди
- можливість завдання серйозної шкоди (фізичної чи психологічної)

Кримінальний закон України має лише фрагментарне та концептуально неадекватне регулювання doxing.

Потенційно найближчою до регулювання doxing є норма статті 182 "Порушення недоторканності приватного життя" є, оскільки передбачає відповідальність за "незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміна такої інформації". Стаття 182 ККУ частково охоплює об'єктивну сторону doxing через елемент "поширення конфіденційної інформації про особу".

Однак існують критичні розбіжності. По-перше, стаття 182 ККУ не вимагає публічного характеру поширення через ІКТ як кваліфікуючої ознаки, тоді як для doxing це є ключовим елементом. По-друге, відсутня спеціальна мета спонукання третіх осіб до заподіяння шкоди. Стаття 182 ККУ не розрізняє звичайне порушення приватності та цілеспрямоване створення умов для подальшого переслідування постраждалої особи іншими.

Крім того, стаття 182 ККУ не враховує ефект масштабування, характерний для цифрового середовища, коли інформація може миттєво поширитися серед величезної кількості людей. Санкції також можуть бути неадекватними серйозності можливих наслідків doxing.

Норма стаття 163 "Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції" може частково застосовуватися до випадків, коли doxing включає розголошення приватної кореспонденції або телефонних розмов. Однак стаття 163 ККУ зосереджена на порушенні таємниці комунікацій, а не на публічному поширенні різноманітних особистих даних.

Основні недоліки полягають у вузькому розумінні предмета злочину, що обмежується кореспонденцією та комунікаціями, тоді як doxing може включати адреси проживання, фотографії, інформацію про родичів, місце роботи, фінансові дані тощо. Також відсутня мета підбурювання до заподіяння шкоди.

У випадках, коли doxing здійснюється з дискримінаційними мотивами, теоретично може застосовуватися стаття 161 "Порушення рівноправності громадян". Однак ця норма має широкий характер та не враховує специфіку цифрового середовища і механізм дії через публічне поширення особистих даних.

Найсерйознішою проблемою є відсутність розуміння doxing як специфічного способу організації колективного домагання. Існуючі норми ККУ розглядають порушення приватності як пряме завдання шкоди постраждалої особі, тоді як doxing є свого роду підготовчим злочином - він створює умови для подальшого переслідування постраждалої іншими особами.

Відсутні норми, що враховують публічний характер поширення інформації через ІКТ як окрему кваліфікуючу ознаку. Це принципово важливо, оскільки публічність робить інформацію доступною для потенційно необмеженого кола осіб, що кратно збільшує можливості для домагання.

Не враховується лавиноподібний ефект doxing, коли початкове розголошення інформації призводить до масового поширення та використання її різними особами для переслідування постраждалої особи. Існуючі норми не передбачають відповідальності за створення умов для колективного заподіяння шкоди.

Відсутня специфіка гендерного контексту doxing. Також проблематичною є відсутність норм про відповідальність за повторний doxing або систематичне поновлення розголошеної інформації після її видалення.

Санкції за порушення приватності в ККУ розраховані на традиційні форми розголошення інформації і не враховують масштаб можливої шкоди від doxing у цифровому середовищі. Максимальні покарання можуть бути недостатніми.

Кібер-підбурювання до насильства (cyber incitement to violence or hatred), стаття 8

Стаття 8 Директиви передбачає, що “1. Держави-члени забезпечують, щоб навмисне підбурювання до насильства або ненависті, спрямоване проти групи осіб або члена такої групи за ознакою статі шляхом публічного розповсюдження за допомогою ІКТ матеріалів, що містять таке підбурювання, каралося як злочин. 2. Для цілей пункту 1 держави-члени можуть вибрати покарання лише за поведінку, яка або здійснюється таким чином, що може порушити громадський порядок, або яка є загрозовою, грубою чи образливою”.

Ключовими елементами кібер-підбурювання згідно з Директивою є:

- дії у вигляді підбурювання до насильства або ненависті
- спрямованість проти групи осіб або її члена такої групи за ознакою статі
- публічне поширення через ІКТ
- умисний характер дій
- дії порушують громадський порядок або є загрозовими, образливими чи принизливими

Норма статті 161 ККУ "Порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками" є найближчою до вимог Директиви щодо кібер-підбурювання. Стаття 161 ККУ передбачає відповідальність за *"умисні дії, спрямовані на розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або образа 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, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками"*.

Стаття 161 ККУ частково відповідає вимогам Директиви через включення "статі" як захищеної ознаки та криміналізацію розпалювання ворожнечі за цією ознакою. Це є значною перевагою порівняно з багатьма іншими нормами ККУ, які взагалі не містять ґендерного компоненту.

Однак існують суттєві недоліки в контексті кібер-підбурювання. Стаття 161 ККУ не містить спеціального акценту на використанні ІКТ як засобу вчинення злочину, хоча це може охоплюватися загальним поняттям "умисних дій".

Відсутня конкретизація публічного характеру поширення через цифрові платформи, що є ключовою ознакою кібер-підбурювання. Директива (пункт 26 Преамбули) наголошує, що *“злочин у вигляді кібер-підбурювання до насильства чи ненависті передбачає, що підбурювання виражається не в суто приватному контексті, а публічно за допомогою використання ІКТ. Таким чином, передбачається розповсюдження широкому загалу, що має розумітися як надання за допомогою ІКТ доступу до певного матеріалу, що є підбурюванням до насильства чи ненависті, потенційно необмеженій кількості осіб, а саме надання легкого доступу до матеріалу користувачам загалом, не вимагаючи подальших дій з боку особи, яка надала матеріал, незалежно від того, чи дійсно ці особи мають доступ до відповідної інформації”*.

Проблематичним є також те, що стаття 161 ККУ має досить широке формулювання, яке може ускладнювати кваліфікацію специфічних випадків онлайн-мізоґінії та ґендерно мотивованої ненависті в цифровому просторі. Директива (пункт 25 Преамбули) особливо звертає увагу, що *“легке, швидке та широке поширення мови ненависті через цифровий світ підсилюється ефектом розгальмування в мережі, оскільки передбачувана анонімність в Інтернеті та відчуття безкарності зменшують стриманість людей щодо участі у таких висловлюваннях. Жінки часто стають об’єктом сексистської та мізоґінної ненависті в Інтернеті, який може перерости у злочини на ґрунті ненависті офлайн. Цій поведінці потрібно запобігати або перешкоджати їй на ранній стадії. Висловлювання, що використовуються в такому типі підбурювання, не завжди безпосередньо стосуються статі цільової особи, але про упереджену мотивацію можна зробити висновок із загального змісту чи контексту підбурювання”*. У аналізованій статті ККУ відсутні спеціальні критерії для оцінки контенту в соціальних мережах, форумах та інших цифрових платформах.

Найсерйознішою проблемою є недостатнє врахування специфіки цифрового середовища як унікального простору для поширення ненависті. Інтернет-платформи створюють можливості для швидкого та масштабного поширення ненависницького контенту, утворення "ехо-камер" та радикалізації поглядів, що принципово відрізняється від традиційних способів розпалювання ворожнечі.

Особливо проблематичною є відсутність спеціальних норм про онлайн-мізоґінію як системне явище. Кібер-підбурювання проти жінок часто має специфічні форми - від

закликів до сексуального насильства до пропаганди обмеження прав жінок у суспільстві. Ці прояви мають унікальні характеристики, що потребують спеціального правового регулювання.

ККУ не враховує феномен інтерсекційної дискримінації в цифровому просторі, коли жінки можуть стати об'єктом ненависті одночасно за кількома ознаками - стать у поєднанні з расою, релігією, сексуальною орієнтацією тощо. Це створює особливо токсичне середовище для окремих груп жінок.

Відсутні норми, що враховують роль алгоритмів соціальних мереж у поширенні ненависницького контенту. Сучасні технології можуть автоматично посилювати розповсюдження матеріалів, що підбурюють до ґендерної ненависті, створюючи ефект штучної ампліфікації.

Кібер-підбурювання часто здійснюється анонімними або псевдонімними акаунтами, що ускладнює ідентифікацію правопорушників. Існуючі норми ККУ не містять спеціальних механізмів для боротьби з анонімним розпалюванням ненависті в цифровому просторі.

Проблематичними є також координовані кампанії ненависті, коли множина акаунтів одночасно поширює схожий контент проти конкретних жінок або груп жінок. Такі "ботоферми" та координовані атаки потребують специфічних правових механізмів протидії.

Сучасні форми кібер-підбурювання використовують складні технологічні рішення - від deepfake відео до AI-генерованого контенту, що містить заклики до ненависті. ККУ не має норм для регулювання цих новітніх технологічних проявів дискримінації.

Санкції за статтею 161 ККУ можуть бути недостатніми для запобігання систематичному кібер-підбурюванню, особливо коли воно здійснюється організованими групами або з використанням комерційних ботомереж.

Також до випадків кібер-підбурювання може частково застосовуватися норма статті 300 ККУ "Ввезення, виготовлення, розповсюдження творів, що пропагують культ насильства і жорстокості", коли контент прямо пропагує насильство проти жінок або містить заклики до жорстоких дій за ознакою статі. Стаття 300 ККУ передбачає відповідальність за "ввезення, виготовлення, розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію".

Перевагою є включення понять "нетерпимість та дискримінація", що може охоплювати ґендерно мотивовані матеріали. Однак стаття не містить прямого посилання на стать як захищену ознаку, що створює прогалини в застосуванні.

Основний недолік полягає в тому, що стаття 300 ККУ зосереджена на "творах" у традиційному розумінні, тоді як кібер-підбурювання часто відбувається через короткі повідомлення, меми, коментарі та інші форми цифрового контенту, які важко підвести під поняття "творів".

3. Інші критичні прогалини

Жіноче обрізання (female genital mutilation), стаття 3

Стаття 3 Директиви ЄС криміналізує:

(а) вирізання, інфібуляцію або будь-яке інше калічення всієї або будь-якої частини великих, малих статевих губ або клітора;

(б) примушування або спонукання жінки чи дівчини до виконання будь-яких дій, зазначених у пункті (а).

При цьому, “термін “видалення” стосується часткового або повного видалення клітора та великих статевих губ. Термін “інфібуляція” стосується закриття великих статевих губ шляхом часткового зшивання зовнішніх губ вульви з метою звуження отвору піхви. Термін “нанесення іншого ушкодження, що призводить до каліцтва” стосується всіх інших фізіологічних змін жіночих статевих органів” (пункт 15 Преамбули Директиви).

Ключовими елементами складу злочину згідно з Директивою є:

- дії у вигляді калічення жіночих геніталій (видалення, інфібуляція, інше калічення)
- примушування або схиляння до таких дій
- спрямованість виключно проти жінок та дівчат
- умисний характер дій
- максимальне покарання не може бути менше 5 років позбавлення волі

Калічення жіночих геніталій теоретично може кваліфікуватися за статтею 121 “Умисне тяжке тілесне ушкодження”, оскільки такі дії часто призводять до тяжких тілесних ушкоджень.

Калічення геніталій відповідає критеріям тяжких тілесних ушкоджень через втрату функцій органів, непоправне знівечення та стійкий розлад здоров'я. Санкції за статтею 121 ККУ (від 5 до 8 років позбавлення волі) формально відповідають мінімальним вимогам Директиви.

Однак застосування цієї норми до жіночого обрізання має принципові недоліки. По-перше, стаття 121 ККУ не враховує специфічну природу калічення жіночих геніталій як форми гендернозумовленого насильства. Це не випадкове тілесне ушкодження, а систематична практика, спрямована на контроль жіночої сексуальності та підпорядкування жінок.

По-друге, відсутній культурний та релігійний контекст, який часто супроводжує жіноче обрізання. Ці злочини вчиняються не з мотивів особистої ворожнечі, а як частина традиційних практик, що вимагає спеціального підходу до кваліфікації та покарання.

По-третє, стаття 121 ККУ не захищає специфічно жінок та дівчат як вразливу групу, тоді як жіноче обрізання є формою дискримінації за ознакою статі.

Менш інвазивні форми жіночого обрізання теоретично можуть кваліфікуватися за статтею 122 ККУ. Однак санкції за цією статтею не відповідають мінімальним вимогам Директиви.

Крім того, кваліфікація жіночого обрізання як "середньої тяжкості" ушкоджень не відображає серйозності цього злочину та його довготривалих наслідків для здоров'я жінок.

Пункт 16 Директиви виділяє унікальні характеристики жіночого обрізання, що принципово відрізняють його від більшості тілесних ушкоджень:

- є формою ґендерного насильства, спрямованого виключно проти жінок та дівчат. Це не просто тілесне ушкодження, а специфічна практика контролю жіночої сексуальності та репродуктивних прав;
- має глибокі культурні, релігійні та соціальні корені в певних спільнотах. Воно часто сприймається не як насильство, а як "традиція" або "обов'язок", що потребує спеціальних підходів до профілактики та покарання.
- має специфічні довготривалі наслідки для фізичного та психологічного здоров'я жінок, включаючи проблеми з пологами, сексуальними відносинами, психічними травмами.

ККУ не містить норм, що враховували б ґендерний характер жіночого обрізання як злочину, спрямованого проти жінок саме через їхню стать, та не розглядає його як форму дискримінації, що обмежує права жінок на тілесну недоторканність і репродуктивне здоров'я. Якщо Директива передбачає широкий спектр форм калічення від повного видалення до символічних процедур, тоді як ККУ не має диференційованого підходу залежно від інвазивності та наслідків. Постраждалі та свідки часто належать до закритих спільнот і потребують спеціальних заходів захисту від тиску або погроз, що не передбачені загальними нормами ККУ.

Санкції за загальні тілесні ушкодження не відповідають унікальній серйозності жіночого обрізання. Директива встановлює мінімум 5 років позбавлення волі, визнаючи особливу тяжкість цього злочину.

“Враховуючи особливий характер злочину, пов’язаного з жіночим обрізанням, і необхідність забезпечення захисту постраждалих, які зазнають конкретної шкоди внаслідок нього” Директива прямо згадує (пункт 16 Преамбули) цей злочин як окремий у кримінальному законодавстві держав-членів.

Примусовий шлюб (forced marriage), стаття 4

Простий складу злочину “Примушування до шлюбу” (стаття 151-2 ККУ) майже повністю відповідає вимогам статті 4 Директиви ЄС, за винятком особи, на яку безпосередньо спрямоване злочинне посягання. Згідно Директиви ЄС (стаття 4) ними є як “доросла особа”, так і “дитина”, згідно законодавства України - “доросла особа” (частина 1) та “особа, яка не досягла шлюбного віку” (частина 2).

Поняття "особа, яка досягла шлюбного віку" у ККУ визначається не прямою нормою самого Кримінального кодексу, а через відсилання до положень Сімейного кодексу України. Шлюбний вік визначається статтями 22-23 Сімейного кодексу: стаття 22 СК - загальний шлюбний вік (18 років), стаття 23 СК - можливість зниження до 16 років.

Стаття 10 (3) Директиви за такий злочин вимагає верхню межу санкції у вигляді позбавлення волі у розмірі щонайменше три роки (тобто мінімум 3 роки, але може бути й більше). Частина 1 статті 151-2 ККУ передбачає позбавлення волі на строк до трьох років (тобто максимум 3 роки), що формально відповідає встановленому Директивою мінімуму.

Однак, стаття 151-2 ККУ дозволяє також альтернативні види покарання - арешт на 6 місяців або обмеження волі, що не є позбавленнями волі в розумінні Директиви та є значно м'якшими за її вимоги. Таким чином, законодавство України не відповідає мінімальним вимогам Директиви щодо суворості покарання за примусовий шлюб.

Враховуючи те, що постраждалі від примусового шлюбу часто є неповнолітніми, Директива ЄС вимагає, щоб строки давності притягнення до кримінальної відповідальності за такий злочин охоплювали такий часовий період, який буде достатнім і співрозмірним із тяжкістю вчиненого правопорушення, щоб забезпечити ефективний початок провадження після того, як постраждала особа досягла 18 років. Частина 6 статті 49 ККУ забезпечує базову відповідність вимогам Директиви.

Обтяжуючі обставини (стаття 11 Директиви)

Стаття 11 Директиви встановлює, що державі-члени повинні забезпечити можливість визнання певних обставин обтяжуючими відповідно до національного права, якщо вони не є складовими елементами кримінальних правопорушень, передбачених статтями 3-8 Директиви.

Директива визначає як обтяжуючу обставину вчинення правопорушення *"проти особи, яка стала вразливою через певні обставини, такі як ситуація залежності або наявність фізичного, психічного, інтелектуального або сенсорного порушення"*, що частково відповідає пункту 6 статті 67 ККУ щодо осіб похилого віку, осіб з інвалідністю або осіб, що перебувають у безпорадному стані. Однак українська норма не охоплює всі категорії вразливих осіб, передбачені Директивою.

Директива передбачає як обтяжуючу обставину вчинення правопорушення *"щодо колишнього або теперішнього подружжя чи партнера"*. Хоча стаття 67 ККУ містить пункт 6-1 про вчинення кримінального правопорушення щодо подружжя чи колишнього подружжя, формулювання потребує уточнення для повного відповідності вимогам Директиви.

Така обставина як *"вчинення правопорушення членом сім'ї або особою, що проживає разом з потерпілим"* частково охоплюється українським законодавством через пункт 6-1, однак потребує розширення для включення всіх категорій, передбачених Директивою.

Істотною прогалиною є відсутність в статті 67 ККУ такої обтяжуючої обставини, передбаченої Директивою *"намір правопорушення зберегти або відновити так звану 'честь' особи, сім'ї, спільноти"*.

Директива встановлює як обтяжуючу обставину *"намір правопорушення покарати потерпілого за сексуальну орієнтацію, гендер, колір шкіри, релігію, соціальне походження або політичні переконання потерпілого"*. Стаття 67 ККУ у пункті 3 частково охоплює це положення через вчинення кримінального правопорушення на ґрунті расової, національної, релігійної ворожнечі чи розбрату або на ґрунті статевої приналежності, однак не включає всі мотиви, передбачені Директивою.

Порівняння всіх обтяжуючих обставин коротко подане у Додатку В.

Із зазначеного випливає, що кримінальне законодавство України містить такі основні прогалини у регулюванні обтяжуючих обставин у справах ґендерно обумовленого насильства, який передбачений Директивою ЄС:

1. відсутність спеціальних ґендерно-чутливих обтяжуючих обставин
2. недостатнє врахування специфіки відносин між правопорушником і постраждалою особою
3. неадекватне регулювання мотивів, пов'язаних з "честю" та дискримінацією

Окремі інші вимоги Директиви

Онлайн-звернення постраждалих осіб (стаття 23 Директиви)

Стаття 14 Директиви вимагає, щоб держави-члени забезпечили можливість постраждалим повідомляти про випадки насильства через доступні, безпечні та легкодоступні онлайн-канали з можливістю подавати докази за допомогою ІКТ. Пункт 30 преамбули Директиви уточнює, що постраждалі повинні мати можливість завантажувати матеріали, що стосуються їх повідомлення, наприклад знімки екрана, що підтверджують ймовірні насильницькі дії. Це має стосуватися принаймні кіберзлочинів, визначених статтями 5-8 Директиви. Стаття 23 вимагає створення механізмів оперативного видалення такого контенту шляхом видачі компетентними органами обов'язкових розпоряджень провайдерам хостингових послуг з дотриманням процедурних гарантій та права на судовий захист для всіх залучених сторін.

Аналіз діючого українського законодавства виявляє суттєві прогалини у виконанні вимог Директиви. Воно не містить положень щодо кіберформ насильства та механізмів онлайн-звернень постраждалих осіб. ККУ не передбачає спеціальних складів злочинів, які повністю відповідали б визначеним Директивою кібер-переслідуванню, поширенню інтимних або зманіпульованих матеріалів без згоди, кібер-домаганням або кібер-підбурюванню до насильства чи ненависті в тому вигляді, як вони визначені Директивою. Хоча Департамент кіберполіції має систему електронних звернень за адресою ticket.cyberpolice.gov.ua, вона не

спеціалізується на захисті постраждалих від домашнього та гендернозумовленого насильства, не інтегрована з системою протидії домашньому насильству та не забезпечує комплексного підходу з координацією соціальних служб, психологів та інших служб підтримки.

Хоча з грудня 2021 року функціонує сайт 1547.ukc.gov.ua для онлайн-звернень, **він не є спеціалізованою платформою для кібернасильства** і не передбачає можливості завантаження електронних доказів (відео, аудіо) у первинному форматі, що є критично важливим для розслідування кіберзлочинів. Система функціонує відповідно до загальних вимог Закону "Про звернення громадян" та постанови КМУ № 976 від 27.11.2019, а не як спеціалізований механізм протидії кібернасильству з можливістю збереження цифрових доказів у форматі, придатному для кримінального процесу.

Для реалізації вимог Директиви Закон "Про запобігання та протидію домашньому насильству" слід доповнити положеннями про право постраждалих звертатися через спеціалізовану онлайн-платформу з можливістю завантаження електронних доказів, при цьому онлайн-звернення повинні мати таку ж юридичну силу, як письмові заяви. Також необхідно створити єдину інтегровану онлайн-платформу для звернень постраждалих від домашнього та гендернозумовленого насильства, яка об'єднає функціонал кіберполіції з системою протидії домашньому насильству та забезпечить автоматичну координацію між правоохоронними органами, соціальними службами, психологами та медичними закладами.

Швидке видалення шкідливого контенту (пункти пункти 51-54, 86 Преамбули, стаття 23 Директиви)

Стаття 23 Директиви деталізує принципи, закладені у пунктах 51-54 та 86 Преамбули, створюючи конкретні правові механізми для негайного видалення онлайн-матеріалів у справах про кібернасильство. Директива встановлює зобов'язання держав-членів забезпечити швидке видалення або блокування доступу до шкідливого контенту, що стосується поширення інтимних або зманіпульованих матеріалів без згоди, кібер-домагання, кібер-переслідування та кібер-підбурювання до насильства чи ненависті.

Центральним механізмом є система обов'язкових розпоряджень компетентних органів, адресованих насамперед постачальникам послуг хостингу. У випадках, коли видалення неможливе через технічні або юридичні перешкоди, органи влади отримують право видавати розпорядження про блокування доступу іншим постачальникам посередницьких послуг, які мають технічні можливості для таких заходів.

Директива встановлює строгі процедурні гарантії, включаючи обов'язкове дотримання стандартів Регламенту (ЄС) 2022/2065 про цифрові послуги, що забезпечує координацію з існуючою європейською системою регулювання онлайн-контенту. Передбачається право на ефективний судовий захист для всіх сторін, включаючи постачальників послуг та авторів

контенту, з можливістю оскарження розпоряджень у судах держави-члена, компетентний орган якої видав розпорядження.

Особливою гарантією є принцип збереження доказів, згідно з яким видалення контенту не повинно перешкоджати компетентним органам отримувати необхідні докази для розслідування злочинів. Також передбачається автоматичне анулювання розпоряджень при припиненні кримінального провадження без встановлення факту злочину, що захищає від необґрунтованого обмеження доступу до інформації.

Вимога прозорості включає обов'язкове інформування постачальників контенту про причини видалення та можливості судового захисту, що забезпечує баланс між швидкістю реагування на кібернасильство та захистом основних прав усіх учасників процесу.

Найсерйознішою прогалиною є повна відсутність у КПКУ процедур негайного видалення онлайн-контенту у справах про гендернозумовлене насильство. Наявні норми про тимчасовий доступ до речей та документів не адаптовані для цифрових матеріалів і не передбачають можливості одночасного зберігання доказів та видалення з публічного доступу. Статті 36, 40 та 40-1 КПКУ про повноваження прокурорів, слідчих та дізнавачів не включають права на видачу розпоряджень про видалення контенту.

Законодавство про електронні комунікації не встановлює обов'язків провайдерів щодо виконання розпоряджень компетентних органів у справах про кібернасильство. Існуючі механізми блокування через НЦУ та НКЕК призначені для фішингових сайтів та не адаптовані для випадків неконсенсуального поширення інтимних матеріалів чи кіберпереслідування.

Процедурні гарантії також є недостатніми. Стаття 303 КПКУ про оскарження дій під час досудового розслідування не передбачає спеціальних механізмів для швидкого судового розгляду оскаржень розпоряджень про видалення контенту. Відсутні норми про автоматичне анулювання таких розпоряджень при припиненні кримінального провадження.

Координація з міжнародними платформами практично неможлива через відсутність правових механізмів взаємодії з постачальниками послуг хостингу за межами України. Це створює особливі труднощі, оскільки більшість випадків кібернасильства відбувається на міжнародних платформах.

Для приведення у відповідність необхідні фундаментальні зміни до КПКУ з додаванням спеціальної глави про тимчасові заходи у справах про кібернасильство, модернізація законодавства про електронні комунікації та створення спеціальних процедур координації з міжнародними інтернет-платформами.

Координація з ІТ-сектором (стаття 42 Директиви)

Стаття 42 Директиви ЄС 2024/1385 зобов'язує держави-члени:

заохочувати саморегулюючу співпрацю між відповідними провайдерами посередницьких послуг, зокрема через створення кодексів поведінки;

підвищувати обізнаність про заходи саморегулювання, прийняті провайдерами посередницьких послуг, особливо щодо:

- посилення механізмів для боротьби з онлайн-матеріалами
- покращення навчання співробітників щодо запобігання правопорушенням та допомоги постраждалим

Додатково, стаття 34, пункт 8 також підтримує цю співпрацю:

“Держави-члени сприяють міждисциплінарному співробітництву та співробітництву між зацікавленими сторонами, у тому числі між відповідними провайдерами посередницьких послуг та компетентними органами, для розробки та впровадження заходів для боротьби з кіберзлочинами, описаними у статтях 5-8”.

Таким чином, Директива заохочує створення механізмів саморегулювання та співпраці між інтернет-провайдерами для ефективної боротьби з кібернасильством. Вітчизняні механізми співпраці з ІТ-сектором існують у контексті модерації воєнного контенту, захисту інтелектуальної власності та блокування санкційних ресурсів. Однак **спеціалізовані механізми співпраці у сфері боротьби з кібернасильством, зокрема щодо негайного видалення інтимних матеріалів, кіберпереслідування та інших форм ґендернозумовленого кібер-насильства, відсутні**. Відсутність формалізованих процедур співпраці з соціальними мережами, месенджерами та іншими онлайн-платформами ускладнює оперативне реагування на випадки кібернасильства. Потреба у створенні спеціальних угод про співпрацю між державними органами та приватними ІТ-компаніями залишається нагальною.

Виклики імплементації

Правові виклики

Найбільш критичним правовим викликом є необхідність доповнення ККУ новими статтями про кібернасильство. За результатами аналізу українського законодавства та вимог Директиви, потрібно додати нові статті, які будуть охоплювати такі види злочинів як кібер-переслідування, кібер-домагання, поширення інтимних матеріалів без згоди та кібер-підбурювання до насильства або ненависті.

Паралельно з криміналізацією нових видів насильства необхідно внести суттєві зміни до Кримінального процесуального кодексу України щодо процедур розслідування злочинів у кіберпросторі. Це включає розробку спеціальних процедур збору та дослідження цифрових доказів, механізмів міжнародного співробітництва у сфері кіберзлочинності та процедур забезпечення анонімності постраждалих осіб під час судового розгляду.

Особливої уваги потребує розробка підзаконних актів, які регламентуватимуть швидке реагування на шкідливий онлайн-контент. Директива вимагає створення механізмів термінового видалення матеріалів, що становлять загрозу для постраждалих від насильства осіб, протягом 24 годин з моменту повідомлення. Це потребує детального правового регулювання взаємодії між правоохоронними органами, судовою системою та інтернет-провайдерами.

Технологічні виклики

Створення систем автоматичного виявлення шкідливого контенту є одним з найскладніших технологічних завдань імплементації. Такі системи повинні використовувати передові технології штучного інтелекту та машинного навчання для ідентифікації образливих зображень, текстів та відео контенту у режимі реального часу. При цьому критично важливо забезпечити баланс між ефективністю виявлення та мінімізацією помилкових спрацьовувань, які можуть призвести до необґрунтованого обмеження свободи слова.

Розвиток безпечних каналів зв'язку для постраждалих від насильства передбачає створення захищених платформ для звернення по допомогу, консультацій та підтримки. Ці канали повинні гарантувати повну конфіденційність та анонімність користувачів, використовуючи сучасні технології шифрування та захисту персональних даних. Особливо важливим є забезпечення доступності таких каналів через різні пристрої та платформи.

Забезпечення технічних можливостей для швидкого видалення контенту вимагає створення автоматизованих систем взаємодії між різними онлайн-платформами та державними органами. Це включає розробку єдиних протоколів обміну інформацією, API для інтеграції з соціальними мережами та іншими інтернет-сервісами, а також систем моніторингу ефективності видалення контенту.

Інституційні виклики

Підготовка кваліфікованих кадрів у сфері кібербезпеки та протидії гендерному насильству є фундаментальним викликом, який вимагає комплексного підходу до освіти та професійного розвитку. Необхідно розробити спеціальні освітні програми для правоохоронців, суддів, прокурорів та соціальних працівників, які охоплюватимуть як технічні аспекти кіберзлочинності, так і гендерно-чутливі підходи до роботи з потерпілими.

Створення спеціалізованих підрозділів кіберполіції потребує не лише фінансування та технічного обладнання, а й розробки нових організаційних структур та процедур роботи. Ці підрозділи повинні мати достатні повноваження та ресурси для ефективного розслідування кібернасильства, включаючи можливості міжнародного співробітництва та доступ до сучасних технологій розслідування.

Розвиток координації між державними органами та приватним сектором вимагає створення нових механізмів партнерства, які б забезпечували ефективний обмін інформацією та координацію дій при реагуванні на випадки кібернасильства. Це включає розробку протоколів взаємодії з інтернет-провайдерами, соціальними мережами та іншими технологічними компаніями.

Соціокультурні виклики

Низький рівень обізнаності суспільства про кібернасильство залишається однією з основних перешкод для ефективної протидії цьому явищу. Багато громадян не усвідомлюють серйозності онлайн-насильства та не знають, як захистити себе від таких загроз або куди звертатися за допомогою. Це вимагає масштабних інформаційних кампаній та освітніх програм для різних вікових груп.

Стереотипи щодо “несерйозності” онлайн-насильства глибоко вкорінені у суспільній свідомості та часто поширюються навіть серед правоохоронців та представників судової системи. Подолання цих стереотипів потребує системної роботи з формування нового розуміння кібернасильства як серйозної загрози, яка може мати такі ж травматичні наслідки, як і фізичне насильство.

Недостатня цифрова грамотність потенційних постраждалих осіб, особливо серед вразливих груп населення, створює додаткові ризики стати постраждалим від кібернасильства. Жінки похилого віку, особи з інвалідністю та представники інших вразливих груп часто не мають достатніх знань про безпеку в інтернеті та способи захисту своїх персональних даних.

Вирішення цих викликів потребує координованих зусиль з боку держави, громадянського суспільства та приватного сектору, а також значних інвестицій у технологічну інфраструктуру, освіту та підготовку кадрів. Успішна імплементація Директиви може стати важливим кроком на шляху до створення безпечного цифрового середовища для всіх громадян України.

Додаток А. Порівняльна таблиця відповідності норм ККУ вимогам Директиви стосовно криміналізації

Стаття Директиви	Склад правопорушення згідно Директиви	Мінімальний строк верхньої межі покарання у вигляді позбавлення волі (ст.10), років	Відповідні норми ККУ	Рівень відповідності	Основні прогалини
Стаття 3 Жіноче обрізання (Female genital mutilation)	(а) вирізання, інфібуляція або будь-яке інше калічення всієї або будь-якої частини великих, малих статевих губ або клітора	5	121 “Умисне тяжке тілесне ушкодження” 122 “Умисне середньої тяжкості тілесне ушкодження”	Частково	Відсутність спеціального складу Ігнорування ґендерного характеру Неадекватні санкції (стосовно 122)
	(б) примушування або спонукання жінки чи дівчини до виконання будь-яких дій, зазначених у пункті (а)	5	121 “Умисне тяжке тілесне ушкодження” 122 “Умисне середньої тяжкості тілесне ушкодження”	Частково	Відсутність спеціального складу Ігнорування ґендерного характеру Неадекватні санкції (стосовно 122)
Стаття 4 Примусовий шлюб (Forced marriage)	Стаття 4 Примусовий шлюб (а)	3	151-2 “Примушування до шлюбу”	Частково	Відсутність спеціального складу Ігнорування ґендерного характеру Неадекватні санкції (передбачені альтернативні санкції поряд з позбавленням волі)
	Стаття 4 Примусовий шлюб (б)	3	151-2 “Примушування до шлюбу”	Частково	Відсутність спеціального складу

Стаття Директиви	Склад правопорушення згідно Директиви	Мінімальний строк верхньої межі покарання у вигляді позбавлення волі (ст.10), років	Відповідні норми ККУ	Рівень відповідності	Основні прогалини
					Ігнорування гендерного характеру Неадекватні санкції (передбачені альтернативні санкції поряд з позбавленням волі)
Стаття 5 Поширення інтимних або оброблених матеріалів без згоди (Non-consensual sharing of intimate or manipulated material)	(а) оприлюднення за допомогою ІКТ зображень, відео чи подібного матеріалу, що зображує відверті дії сексуального характеру або інтимні частини тіла особи, без згоди цієї особи, якщо такі дії можуть завдати серйозної шкоди цій особі;	1	182 “Порушення недоторканності приватного життя” 163 “Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер” 301 “Ввезення, виготовлення, збут і розповсюдження порнографічних предметів” 301-1 ККУ “Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше	Частково	Відсутність спеціального складу Ігнорування гендерного характеру Неврахування ІКТ-специфіки Неадекватні санкції (передбачені альтернативні санкції поряд з позбавленням волі)

Стаття Директиви	Склад правопорушення згідно Директиви	Мінімальний строк верхньої межі покарання у вигляді позбавлення волі (ст.10), років	Відповідні норми ККУ	Рівень відповідності	Основні прогалини
			переміщення, виготовлення, збут і розповсюдження” 301-2 ККУ “Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи” попри те, що їх склади прямо передбачають використання інформаційно-телекомунікаційних систем чи технологій		
	(b) виробництво, обробка, внесення змін та подальше оприлюднення за допомогою ІКТ зображень, відео чи подібного матеріалу, що створює враження, ніби особа бере участь у відверто сексуальних діях, без згоди цієї особи, якщо такі дії можуть завдати серйозної шкоди цій особі;	1	182 “Порушення недоторканності приватного життя” 301 “Ввезення, виготовлення, збут і розповсюдження порнографічних предметів”	Слабко	Відсутність спеціального складу Ігнорування гендерного характеру Неврахування ІКТ-специфіки Немає норм про deepfakes Неадекватні санкції (передбачені альтернативні санкції поряд з позбавленням волі)

Стаття Директиви	Склад правопорушення згідно Директиви	Мінімальний строк верхньої межі покарання у вигляді позбавлення волі (ст.10), років	Відповідні норми ККУ	Рівень відповідності	Основні прогалини
	(с) погроза вчинення дій, зазначених у підпункті (а) або (b), з метою примусити особу вчинити, мовчки погодитися або утриматися від певної дії	1	182 “Порушення недоторканності приватного життя” 163 “Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер”	Слабко	Відсутність спеціального складу Ігнорування ґендерного характеру Неврахування ІКТ-специфіки Відсутність revenge porn складу Неадекватні санкції (передбачені альтернативні санкції поряд з позбавленням волі)
Стаття 6 Кіберпереслідування (Cyber stalking)	неодноразове або постійне спостереження за допомогою ІКТ за особою без її згоди або без законного дозволу на це з метою відстеження або моніторингу пересування та діяльності цієї особи, якщо такі дії ймовірно завдають тяжкої шкоди цій особі, каралися як злочин.	1	182 “Порушення недоторканності приватного життя” 163 “Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер” 361 “Несанкціоноване втручання в роботу інформаційних	Слабко	Відсутність спеціального складу Ігнорування ґендерного характеру Неврахування ІКТ-специфіки Неврахування ознаки систематичності Відсутність поняття stalkerware Неадекватні санкції (передбачені альтернативні санкції

Стаття Директиви	Склад правопорушення згідно Директиви	Мінімальний строк верхньої межі покарання у вигляді позбавлення волі (ст.10), років	Відповідні норми ККУ	Рівень відповідності	Основні прогалини
			(автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж”		поряд з позбавленням волі)
Стаття 7 Кібердомогання (Cyber harassment)	(а) неодноразова або постійна участь у загрозових діях за допомогою ІКТ, спрямованих на особу, принаймні, якщо такі дії включають погрози вчинення кримінальних правопорушень, коли ці дії можуть викликати у цієї особи серйозні побоювання за власну безпеку або безпеку її утриманців;	1	129 ККУ "Погроза вбивством"	Слабко	Відсутність спеціального складу Ігнорування гендерного характеру Неврахування ІКТ-специфіки Немає cyberflashing складу Неадекватні санкції (передбачені альтернативні санкції поряд з позбавленням волі)
	(б) вчинення спільно з іншими особами за допомогою ІКТ публічно доступних погрозових або образливих дій, спрямованих на особу, якщо така поведінка може спричинити серйозну психологічну	1	296 “Хуліганство”	Слабко	Відсутність спеціального складу (норми про групові атаки) Ігнорування гендерного характеру Неврахування ІКТ-

Стаття Директиви	Склад правопорушення згідно Директиви	Мінімальний строк верхньої межі покарання у вигляді позбавлення волі (ст.10), років	Відповідні норми ККУ	Рівень відповідності	Основні прогалини
	шкоду цій особі;				специфіки Неадекватні санкції (передбачені альтернативні санкції поряд з позбавленням волі)
	(с) несанкціоноване надсилання за допомогою ІКТ зображення, відео чи іншого подібного матеріалу із зображенням геніталій особі, якщо така поведінка може спричинити серйозну психологічну шкоду цій особі;		301 "Ввезення, виготовлення, збут і розповсюдження порнографічних предметів"	Дуже Слабо	Відсутність спеціального складу cyberflashing Ігнорування ґендерного характеру Неврахування ІКТ-специфіки Неадекватні санкції (передбачені альтернативні санкції поряд з позбавленням волі)
	(d) оприлюднення за допомогою ІКТ матеріалів, що містять персональні дані особи, без згоди цієї особи з метою спонукання інших осіб завдати цій особі фізичної чи серйозної психологічної шкоди	1	182 "Порушення недоторканності приватного життя" 163 "Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами	Слабо	Відсутність спеціального складу doxing Ігнорування ґендерного характеру Неврахування ІКТ-специфіки Неадекватні санкції (передбачені

Стаття Директиви	Склад правопорушення згідно Директиви	Мінімальний строк верхньої межі покарання у вигляді позбавлення волі (ст.10), років	Відповідні норми ККУ	Рівень відповідності	Основні прогалини
			зв'язку або через комп'ютер 161 “Порушення рівноправності громадян залежно від їх расової, національної, регіональної належності, релігійних переконань, інвалідності та за іншими ознаками”		альтернативні санкції поряд з позбавленням волі)
Стаття 8 Кіберпідбурювання до насильства чи ненависті (Cyber incitement to violence or hatred)	навмисне підбурювання до насильства або ненависті, спрямоване проти групи осіб або члена такої групи за ознакою статі шляхом публічного розповсюдження за допомогою ІКТ матеріалів, що містять таке підбурювання, каралося як злочин	1	161 “Порушення рівноправності громадян залежно від їх расової, національної, регіональної належності, релігійних переконань, інвалідності та за іншими ознаками” 300 “Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію”	Частково	Відсутність спеціального складу Ігнорування гендерного характеру Неврахування ІКТ-специфіки Неадекватні санкції (передбачені альтернативні санкції поряд з позбавленням волі)

Додаток В. Порівняльна таблиця обтяжуючих обставин згідно Директиви ЄС 2024/1385 та ККУ

№	Директива ЄС 2024/1385 (ст. 11)	ККУ (ст. 67)	Тип відповідності
1	Повторне вчинення злочину (злочин або інший злочин проти жінок/домашнього насильства вчинено повторно) (п. “а”)	Повторність та рецидив вчинення злочину особою повторно та рецидив злочинів (п. 1)	☒ ПОВНА АНАЛОГІЯ
2	Вразливість потерпілого вчинення проти особи, яка стала вразливою через певні обставини (залежність, або наявність фізичного, психічного, інтелектуального або сенсорного порушення) (п. “b”)	Вразливий стан потерпілого проти особи похилого віку, з інвалідністю, в безпорадному стані, з психічним розладом (п. 6)	♦ ЧАСТКОВА АНАЛОГІЯ (не охоплює всі категорії вразливих осіб, передбачені Директивою)
3	Проти дитини злочин вчинено щодо дитини (п. “с”)	Проти малолітньої дитини вчинення щодо малолітньої дитини (п. 6)	♦ ЧАСТКОВА АНАЛОГІЯ (різний віковий діапазон)
4	В присутності дитини злочин вчинено в присутності дитини (п. “d”)	В присутності дитини вчинення у присутності дитини (п. 6)	☒ ПОВНА АНАЛОГІЯ
5	Групове вчинення злочин вчинено двома або більше особами спільно (п. “e”)	Група за попередньою змовою вчинення групою осіб за попередньою змовою (п. 2)	♦ ЧАСТКОВА АНАЛОГІЯ (різні вимоги до змови)
6	Екстремальне насильство злочину передувало насильство надзвичайного рівня або ж злочин супроводжувався	✗ ВІДСУТНЄ	✗ ВІДМІННІСТЬ Україна не має цієї обставини

	наси́льством надзвичайного рівня (п. “f”)		
7	Використання зброї вчинення з використанням зброї або з погрозою використання зброї (п. “g”)	✗ ВІДСУТНЄ	✗ ВІДМІННІСТЬ Україна не має цієї обставини
8	Застосування сили/примусу вчинення з використанням сили або з погрозою застосування сили примусу (п. “h”)	✗ ВІДСУТНЄ (як са́мостійна обставина)	✗ ВІДМІННІСТЬ
9	Смерть або серйозна шкода дії спричинили смерть постраждалої особи або тяжку фізичну чи психологічну шкоду постраждалій особі (п. “i”)	Тяжкі наслідки тяжкі наслідки, завдані злочином (п. 5)	☒ ПОВНА АНАЛОГІЯ
10	Попередні засудження правопорушник був раніше судимий за злочини того ж характеру (п. “j”)	Рецидив рецидив злочинів (п. 1)	☒ ПОВНА АНАЛОГІЯ
11	Подружжя/партнер вчинення проти колишнього або теперішнього подружжя чи партнера (п. “k”)	Подружжя та близькі проти подружжя, колишнього подружжя або інших осіб у сімейних/ близьких відносинах (п.6 ¹)	☒ ПОВНА АНАЛОГІЯ
12	Член сім'ї/співмешканець вчинення членом сім'ї постраждалої особи або особою, яка проживає з нею (п. “l”)	Сімейні/близькі відносини проти осіб у сімейних або близьких відносинах (п.6 ¹)	☒ ПОВНА АНАЛОГІЯ

13	Зловживання довірою вчинення шляхом зловживання визнаною довірою, владою або впливом (п. "m")	Службова/матеріальна залежність проти особи, яка перебуває в матеріальній, службовій чи іншій залежності (п. 8)	♦ ЧАСТКОВА АНАЛОГІЯ (схожа концепція, різні формулювання)
14	Публічні особи вчинення проти особи через те, що ця особа є громадським представником, журналістом або правозахисником (п. "n")	Службовий/громадський обов'язок у зв'язку з виконанням потерпілим службового або громадського обов'язку (п. 4)	♦ ЧАСТКОВА АНАЛОГІЯ (схожа концепція, різний обсяг)
15	"Чесць" родини/спільноти намір зберегти або відновити так звану "чесць" особи, сім'ї, громади чи іншої подібної групи (п. "o")	✗ ВІДСУТНЄ	✗ ВІДМІННІСТЬ
16	Дискримінаційні мотиви намір покарати постраждалу особу за сексуальну орієнтацію, гендер, колір шкіри, релігію, соціальне походження чи політичні переконання (п. "p")	Дискримінаційні мотиви на ґрунті расової, національної, релігійної ворожнечі або на ґрунті статевої приналежності (п. 3)	♦ ЧАСТКОВА АНАЛОГІЯ Норма Директиви робить акцент на на мотиві "помсти/покарання", а також містить три додаткові захищені ознаки, а саме: сексуальна орієнтація, соціальне походження, політичні переконання

Українська національна платформа Форуму громадянського суспільства Східного партнерства – це мережа з понад 150 громадських організацій України, що відстоюють українські інтереси в рамках Східного партнерства. Платформа є частиною Форуму громадянського суспільства Східного партнерства (ФГС СхП).

Форум громадянського суспільства Східного партнерства – унікальна багаторівнева регіональна платформа громадянського суспільства, спрямована на просування європейської інтеграції, сприяння реформам та демократичним перетворенням у шести країнах Східного партнерства – Вірменії, Азербайджані, Білорусі, Грузії, Молдові та Україні. Будучи громадським елементом СхП, ФГС СхП намагається посилити громадянське суспільство у регіоні, підвищити рівень плюралізму у публічному дискурсі та політиці шляхом сприяння демократії участі та фундаментальних свобод. ФГС СхП – це позапартійна добровільна неурядова організація.

Українська національна платформа Форуму громадянського суспільства Східного партнерства:

eap-csf.org.ua

unp.eap@gmail.com

www.facebook.com/unp.eap.csf

ГО Центр “Жіночі перспективи”

women.lviv.ua

women@women.lviv.ua

www.facebook.com/ZahidnoukrainskijCentrZinociPerspektivi

