ПРОТИДІЯ КІБЕРБУЛІНГУ ТА КІБЕРГРУМІНГУ В УКРАЇНІ

Попередній аналітичний огляд

Богдан Мойса, аналітик правозахисного департаменту «Docudays UA»

Зміст

Вступ

Інформаційні технології, що стрімко розвиваються, мають сильний вплив на права людини, зокрема дітей, даючи широкі можливості для освіти, розвитку, участі та висловлення поглядів. Водночас їх використання призводить до серйозних ризиків насильства, експлуатації та іншого неналежного поводження. Адекватне та ефективне реагування на ці ризики – предметом уваги міжнародних та регіональних організацій. Інформаційний простір України рясніє повідомленнями про знущання над дітьми через соціальні мережі, використання сервісів для сексуальної експлуатації дітей.

Застосування засобів електронної комунікації стало складовою частиною визначення булінгу в національному законодавстві, однак питання ефективного реагування на кібербулінг залишається відкритим.

У національному законодавстві не імплементовано статтю 23 Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства, у межах якої визначено необхідність встановлення відповідальності за грумінг за допомогою інформаційно-комунікаційних технологій.

Мета огляду – окреслення стану справ з протидії кібербулінгу та кібергрумінгу в Україні на основі аналізу відповідності національного законодавства міжнародним та регіональним стандартам.

Приділено увагу огляду міжнародних та регіональних стандартів захисту прав дітей у цифровому середовищі. Зокрема стандартів Конвенції про права дитини та інших інституцій і механізмів ООН. Виокремлено практику та керівні принципи інституцій Ради Європи у сфері захисту прав дітей у середовищі інформаційних технологій. Проглянуто й національне право та його імплементацію, зокрема, через аналіз судової практики з протидії булінгу.

Для цілей попереднього аналітичного огляду терміни «кібербулінг» та «кібергрумінг» вживатимуться в таких значеннях:

Кібербулінг – агресивний, навмисний акт, учинений однією особою або групою осіб з використанням електронних форм стосовно жертви, якій важко захистити себе. Зазвичай здійснюється неодноразово за певний період часу та характеризується нерівністю сил. Кібербулінг може включати поширення слухів, розміщення неправдивої інформації або неприємних повідомлень, коментарів чи фотографій, які принижують, а також виключення будь-кого з онлайн-мереж чи комунікацій.

Кібергрумінг (онлайн-грумінг – це налагодження довірливих стосунків з дитиною (найчастіше через соціальні мережі та фейкові акаунти) для отримання від неї інтимних фото чи відео з подальшим шантажуванням дитини для одержання ще відвертіших матеріалів, грошей чи зустрічей в

офлайні.

Пропонованим попереднім оглядом «DocudaysUA» розпочинає низку досліджень, які б сприяли формуванню ефективної державної політики забезпечення та захисту прав дитини в цифровому середовищі.

1. Ідентифікація та опис проблеми

Численні публікації в ЗМІ, дослідження міжнародних та національних експертів, аналітичних центрів та неурядових організацій свідчать про значну увагу до викликів правам дитини в цифровому середовищі, зокрема, кібербулінгу та кібергрумінгу. Роботи спрямовані як на аналіз цих явищ, їх структурування та причини виникнення, так і на прояви кібербулінгу та кібергрумінгу в Україні.

Аналізуючи явище кібербулінгу, експерти вважають: «Приниження в мережі може бути додатковим до системи реального цькування, що посилює і його вплив на жертву, і його наслідки. А може існувати окремо від реальності, тобто бути самостійним видом переслідування, не пов'язаним зі статусом дитини в реальному житті». Небезпеку кібербулінгу пов'язують з низкою факторів, зокрема, поглибленням інформаційного розриву між батьками та дітьми через недостатні знання батьків щодо інтернет-технологій та сервісів, якими дитина користується, – проста заборона користуванням Інтернетом може лише призвести до інформаційного відчуження дитини від групи однолітків.

Сучасні американські дослідники Робін Ковальскі, С'юзан Лімбер і Патріція Агатстон виокремлюють вісім типів поведінки, що характерні для кібербулінгу й відображають переважну більшість різновидів негативного впливу в інтернет-просторі:

1. Суперечки, або флеймінг (від англ. flaming – пекучий, гарячий, полум'яний) – обмін короткими гнівними й запальними репліками між двома чи більше учасниками за допомогою комунікаційних технологій. Найчастіше розгортається в «публічних» місцях Інтернету, на чатах, форумах, дискусійних групах, інколи перетворюється в затяжну війну. На перший погляд, флеймінг – це боротьба між рівними, але в певних умовах вона теж може перетворитися на нерівноправний психологічний терор. Так, неочікуваний випад може привести жертву до сильних емоційних переживань, особливо тоді, коли вона не знає, хто серед учасників яку займе позицію, наскільки її позиція буде підтримана значущими учасниками.

2. Нападки, постійні виснажливі атаки (англ. harassment) – найчастіше це

залучення повторюваних образливих повідомлень, спрямованих на жертву (наприклад, сотні смс-повідомлень на мобільний телефон, постійні дзвінки) з перевантаженням персональних каналів комунікації. На відміну від перепалки, атаки більш тривалі й односторонні. В чатах чи на форумах (місця розмов в Інтернеті) нападки теж трапляються, в онлайн-іграх нападки найчастіше використовують гріфери (grieffers) – група гравців, які ставлять собі за мету перемогти в певній грі, руйнуючи ігровий досвід інших учасників.

3. Обмовлення, зведення наклепів (denigration) – розповсюдження принизливої неправдивої інформації з використанням комп'ютерних технологій. Це можуть бути і текстові повідомлення, і фото, і пісні, які змальовують жертву в шкідливій, інколи сексуальній манері. Жертвами можуть ставати не тільки окремі підлітки, трапляється розсилка списків (наприклад, «хто є хто», або «хто з ким спить» у класі, школі), створюються спеціальні «книги для критики» (slam books), у яких розміщуються жарти про однокласників, де також можуть бути наклепи, перетворюючи гумор на техніку «списку групи ненависті», з якого вибираються мішені для тренування власної злоби, зливання роздратування, переносу агресії тощо.

4. Самозванство, втілення в певну особу (impersonation) – переслідувач позиціонує себе як жертву, використовуючи її пароль доступу до її акаунту в соціальних мережах, блогу, пошти, системи миттєвих повідомлень тощо, а потім здійснює негативну комунікацію. Організація «хвилі зворотних зв'язків» відбувається, коли з адреси жертви без її відому відправляються ганебні провокаційні листи її друзям і близьким за адресною книгою, а потім розгублена жертва неочікувано отримує гнівні відповіді. Особливо небезпечним є використання імперсоналізації проти людей, включених до «списку груп ненависті», адже наражає на реальну небезпеку їхнє життя.

5. Ошуканство, видурювання конфіденційної інформації та її розповсюдження (outing&trickery) – отримання персональної інформації в міжособовій комунікації й передача її (текстів, фото, відео) в публічну зону Інтернету або поштою тим, кому вона не призначалась.

6. Відчуження (остракізм), ізоляція. Будь-якій людині, особливо в дитинстві, притаманно сприймати себе або в якійсь групі, або поза нею. Бажання бути включеним у групу – мотив багатьох вчинків підлітків. Виключення із групи сприймається як соціальна смерть. Що більшою мірою людина виключається із взаємодії, наприклад, у грі, то гірше вона себе почуває й то більше знижується її самооцінка. У віртуальному середовищі виключення також наражає на серйозні емоційні негаразди, аж до повного емоційного руйнування дитини. Онлайн-відчуження можливе в будь-яких типах середовищ, де використовується захист паролями, формується список небажаної пошти або список друзів. Кіберостракізм проявляється також через

відсутність швидкої відповіді на миттєві повідомлення чи електронні листи.

7. Кіберпереслідування – це дії з прихованого вистежування переслідуваних і тих, хто пересувається без діла поруч, зазвичай зроблені нишком, анонімно, для організації злочинних дій на кшталт спроб зґвалтування, фізичного насильства, побиття. Відстежуючи через Інтернет необережних користувачів, злочинець отримує інформацію про час, місце й усі необхідні умови здійснення майбутнього нападу.

8. Хепіслепінг (від англ. happy slapping – щасливе ляскання) – зйомка та поширення відеороликів в яких записано реальні напади. Відеоролики нападів з метою ґвалтування чи його імітації інколи ще називають хопінг – наскок (особливо поширений в США). Ці відеоролики розміщують в Інтернеті, де його можуть продивлятись тисячі людей, зазвичай без жодної згоди жертви. Інша форма хепіслепінгу – це передавання сюжетів через мобільні телефони».

Щодо кібергрумінгу як одного з ризиків в цифровому середовищі, то це явище може відбуватися в інтернет-чатах, соціальних мережах або ігрових сайтах. Хоча акт грумінгу не є новою тактикою, але його використання в Інтернеті створює небезпеку швидкого та анонімного залучення дітей.

Масштабність використання інформаційних технологій для залякування та приниження одних дітей іншими чи групами інших, так само як і в ситуації грумінгу, наявні як в соціологічних дослідженнях, так і кількісних даних, оприлюднених правозахисними інституціями чи неурядовими організаціями. Так, за даними, наведеними «Ла Страда-Україна», із 40 072 дзвінків, що надійшли на гарячу телефонну лінію за 2017–2018 роки, 13381 стосувались небезпеки дітей в Інтернеті (11 581 від дітей, 1800 від дорослих). Зокрема, звернення стосувались: 3095 – комп'ютерна та інтернет-залежність, 2845 – секстинг, 1632 – троллінг, 1385 – грумінг, 1230 – мобінг, 1220 – фішинг, 925 – кібербулінг, 924 – смертельні квести в мережі, 125 – кардинг.

Цінним джерелом щодо позиції дітей та молоді, зокрема питань кібербулінгу, є молодіжний проект U-Report – швидкі опитування через СМС та Твітер, – ініційований ЮНІСЕФ. Не будучи репрезентативним, U-Report все-таки дає можливість простежити певні тенденції вразливості дітей до загроз цифрового середовища. Так, у липні 2016 в межах проекту проводилось опитування за темою «Кібербулінг». Згідно з дослідженням, 30% респондентів з 3836, які відповіли на питання проявів кібербулінгу, стикнулися з плітками та брехнею, 19% зазнавали прямих образ, фото 7% поширювали без їхньої згоди. Водночас 44% з такими випадками не стикалися. Реакцією на кібербулінг стало блокування булера – 49% опитаних, розповісти про ситуацію іншим вирішили 30%. Ще 4% повідомили провайдерів. Водночас 49% респондентів порадили б своїм друзям, що потрапили в цю ситуацію, краще її зігнорувати.

Щодо окремих форм кібербулінгу, то розсилання образливих

повідомлень стало предметом опитування «Безпека в інтернеті (кібербулінг)» цього самого проекту. Так, станом на 26 лютого 2019 року, 38% з 15 095 опитаних отримували погрозливі та/або принизливі повідомлення в Інтернеті. Щодо реакцій на такі повідомлення, то 59% опитаних їх ігнорували, 19% блокували особу, яка принижує, 8% залишали скаргу адміністратору соціальної мережі, 7% ображали у відповідь, 5% просили припинити, 1% просили допомогти сторонніх людей. Низький відсоток тих, хто просив допомоги в інших людей, та жодного, хто звернувся до кіберполіції, підтверджує позицію експертів щодо упередженості проти скарг та недовіру до ефективності наявних способів захисту. Опосередкованим підтвердженням цього може слугувати позиція 34% опитаних, які взагалі нікому не розповідали про цю ситуацію. По 1% могли б розповісти шкільному психологу/ психологині та кіберполіції, і жоден не ділився б проблемою з учителем/ вчителькою. Половина опитаних поділилась би нею з друзями. По 6% розповіли б про це батькам та адміністратору соціальної мережі. Ще 3% розповіли своїм підписникам у соціальних мережах. Щодо інших форм кібербулінгу, то дослідження того самого проекту за 2017 рік показує, що 28% з 14 710 опитаних стикнулися із ситуацією, коли особисту інформацію (фото, відео, записи) розповсюджували в Інтернеті (соціальних мережах) без їхньої згоди.

В опитуванні за темою секстингу проекту U-Report узяло участь 25 035 респондентів, 40% з яких надсилали комусь свої фото інтимного змісту. Більшість 62% робили це на прохання партнерів. Однак варто зауважити, що 1% (орієнтовно 90 респондентів) надсилали фото на прохання незнайомої людини. І хоча ця кількість є відносно незначною, така безпечність може призводити до ризиків наразитись на кібергрумінг.

Вразливість до ризиків кібергрумінгу підтверджує ще одне опитування в межах U-Report, проведене у 2017 році. Так, 26% з 17 373 респондентів спілкувались в Інтернеті (соціальних мережах) з незнайомими людьми на особисті теми. 41% робили це для розваги, 16% керувались тим, що незнайомі люди не будуть засуджувати, 12% через проблеми в особистих відносинах, 9% через непорозуміння в сім'ї та 8% через проблеми в стосунках з однолітками.

За даними іншого дослідження «Голоси дітей», проведеного Коаліцією «Права дитини в Україні», 19% дітей стикнулися з булінгом, із них – 22% отримували погрозливі повідомлення в Інтернеті чи соціальних мережах. 7% такі повідомлення отримували телефоном. Загалом участь в опитуванні взяли 1290 дітей.

На жаль, окреслене підтверджує значний ризик благополуччю дітей через кібербулінг, а також їх вразливість до кібергрумінгу. Втрата комунікацій із сім'єю та недовіра до можливостей допомоги, особливо від закладів освіти,

лише посилює ризики безпеки дітей в інформаційному просторі.

2. Національне законодавство та практика його імплементації

Ця частина сфокусована на правових засадах державної політики у сфері, що є предметом огляду, зокрема, оцінено пріоритетність завдань запобігання та протидії кібербулінгу та кібергрумінгу в довгострокових рішеннях, інтегрування цих явищ до національного законодавства, а також практику національних судів з його імплементації.

Стратегічні рамки. Питання забезпечення прав дитини знайшло своє відображення у стратегічних пріоритетах держави у сфері прав людини, зокрема з імплементації міжнародних зобов'язань, а також політики, безпосередньо спрямованої на дітей.

Національною стратегією у сфері прав людини констатовано актуальність проблем експлуатації дітей, а один з її очікуваних результатів передбачає зменшення кількості дітей – жертв експлуатації та насильства. Досягти цього результату планувалося, зокрема, через увідповіднення законодавства з Конвенцією Ради Європи із захисту дітей від сексуальної експлуатації та сексуального насильства, а також через проведення досліджень щодо протидії експлуатації дітей.

Створення безпечного інформаційного простору для дітей визначено одним із пріоритетів Державної соціальної програми «Національний план дій щодо реалізації Конвенції ООН про права дитини» на період до 2021 року. Цей пріоритет включає напрями: забезпечення захисту персональних даних дитини та іншої конфіденційної інформації про неї, забезпечення безпеки дітей в інформаційному просторі; формування політики запобігання проявам радикалізму, расизму, ксенофобії та іншим формам екстремізму в дітей в умовах стрімкого розвитку інформаційних технологій; внесення до освітніх програм для дітей віком від 7 до 14 років та програм підвищення кваліфікації вчителів питань безпеки дітей в інформаційному просторі; впровадження системи соціально-педагогічної роботи з батьками з питань безпеки дітей в інформаційному просторі. Важко оцінити спосіб вимірювання впровадження цього пріоритету через наявність лише одного індикатора до завдання «запобігання проявів радикалізму», а саме: кількості дітей, залучених до міжнародних проектів. До прикладу, не було б зайвим вимірювати кількість освітніх програм із забезпечення та захисту прав дітей в інформаційному середовищі, а також інші моніторингові показники, щодо протидії кібербулінгу та кібергрумінгу.

Заходи ж для реалізації вищезазначених завдань стосуються переважно інформаційної роботи з батьками, дітьми, іншими відповідними стейкхолдерами щодо безпечного інформаційного простору для дітей. Наразі важко зрозуміти, які саме дії мають на увазі розробники програми заходу «32.2. проведення комплексних заходів із запобігання формуванню у дітей проявів радикалізму, расизму, ксенофобії та інших форм екстремізму». Не беручи під сумнів проведення широкомасштабної інформаційної роботи, без більшого розуміння комплексу послуг із запобігання проявів радикалізму пропоновані кроки з реалізації пріоритетів програми виглядають недостатніми. Однак сама наявність цих пріоритетів у політичному порядку денному дозволяє наполягати на їх втіленні.

Ще одним довгостроковим рішенням, план заходів якого може містити кроки з протидії кібербулінгу, є Національна стратегія реформування системи юстиції щодо дітей на період до 2023 року. «Ця Стратегія спрямована на розв'язання основних системних проблем юстиції стосовно дітей, подолання прогалин у системі міжвідомчої взаємодії, забезпечення профілактичної, соціально-виховної роботи та роботи, спрямованої на ресоціалізацію неповнолітніх, які схильні до протиправної поведінки та вчинили правопорушення, а також на посилення захисту прав дітей, які потерпіли від правопорушень, зокрема, насильницького характеру, та дітей, які є свідками правопорушень».

Огляд лише трьох стратегічних документів дозволяє говорити про наявність рамок для формування необхідного правового поля із запобігання та протидії кібербулінгу та кібергрумінгу.

Кібербулінг у правовому полі. З прийняттям Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)» було сформовано відповідну державну політику. Згідно із Законом: «*Булінг (цькування), тобто, діяння учасників освітнього процесу, які полягають у психологічному, фізичному, економічному, сексуальному насильстві, зокрема із застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи або такою особою стосовно інших учасників освітнього процесу, внаслідок чого могла бути чи була заподіяна шкода психічному або фізичному здоров'ю потерпілого*». Пропонований огляд не ставить собі за мету аналіз Закону як такого. Інтерес становить лише його ефективність протидії булінгу в цифровому середовищі.

Ухвалений акт, без сумніву, має важливе значення для зменшення безкарності за переслідування в освітньому середовищі, однак його ефективність протидії переслідуванню з використанням інформаційних технологій наразі оцінити складно. Частину визначення <…> у тому числі із застосуванням засобів електронних комунікацій <…> можна вважати

формальним визнанням кібербулінгу як ризику правам дитини, але чи виглядає це достатнім? Вище згадувалась позиція експертів щодо дуальної природи кібербулінгу. З одного боку, його можна розглядати як продовження булінгу в офлайні. У цьому зв'язку пропоновані заходи протидії працюватимуть, напевне, однаково. Проте, з другого боку, кібербулінг можна розглядати і як самостійне явище, не обов'язково пов'язане з відносинами поза цифровим середовищем. З цієї позиції ефективність запобігання та протидія кібербулінгу визначеними Законом засобами доводиться поставити під сумнів.

Закон певним чином пропонує координацію інституцій з протидії булінгу – заклад освіти, його засновник (переважно орган місцевого самоврядування), органи Національної поліції України, Служби у справах дітей. Проте левова частка заходів запобігання та протидії булінгу лежить саме на закладі освіти. Так, керівник закладу освіти «забезпечує створення у закладі освіти безпечного освітнього середовища, вільного від насильства та булінгу (цькування), у тому числі: розробляє, затверджує та оприлюднює план заходів, спрямованих на запобігання та протидію булінгу (цькуванню) в закладі освіти; розглядає заяви про випадки булінгу (цькування) здобувачів освіти, їхніх батьків, законних представників, інших осіб та видає рішення про проведення розслідування; скликає засідання комісії з розгляду випадків булінгу (цькування) для прийняття рішення за результатами проведеного розслідування та вживає відповідних заходів реагування; забезпечує виконання заходів для надання соціальних та психолого-педагогічних послуг здобувачам освіти, які вчинили булінг, стали його свідками або постраждали від булінгу (цькування); повідомляє уповноваженим підрозділам органів Національної поліції України та службі у справах дітей про випадки булінгу (цькування) в закладі освіти». Чи спроможні заклади освіти реалізувати ці повноваження в ситуації кібербулінгу?

Певні види кібербулінгу можуть відбуватися, по-перше, за межами закладу освіти, по-друге, онлайн-колективи не обов'язково є групою одного й того самого закладу. Виникає й сумнів щодо спроможності системи освіти, зокрема, освітніх закладів запобігати та протидіяти кібербулінгу, сумніви щодо якої фактично підтвердили результати досліджень, наведені в першій частині. Зрештою, чи може заклад провести відповідне розслідування, тим паче, коли йтиметься про види переслідування в цифровому середовищі, пов'язані з персональними даними? Навіть більше, чи зможуть фахівці закладу освіти належно оцінити шкоду, нанесену дитині через, наприклад, соціальні мережі?

На жаль, окреслене не дозволяє говорити про достатність заходів для запобігання та протидії кібербулінгу.

За кілька місяців дії Закону щодо протидії булінгу прийнято низку судових рішень, що дозволяють простежити його ефективність у ситуації

протидії кібербулінгу. Так, станом на 5 квітня 2019 винесено 48 постанов судів відповідно до статті 173.4 Кодексу про адміністративні правопорушення.

Із матеріалів постанов вбачається, що чотири випадки можна трактувати як кібербулінг. Протоколи за двома справами були складені за фактом розповсюдження фото без згоди особи. В одному випадку через viber, у трьох інших – Instagram. Власне, перша судова Постанова від 5 лютого винесена за фактом розповсюдження фото через Instagram. Як приклад однієї зі справ: особа, отримавши згодом видалені фото інтимного характеру, створила фейкову сторінку, через яку розповсюджувала ці фото серед одногрупників потерпілої.

Використання інформаційно-комунікаційних технологій згадувалось у матеріалах ще двох справ. Зокрема, до особи застосовано стягнення у вигляді громадських робіт за вчинену бійку. Проте, зі слів цієї особи, події, що трапилися, були захистом подруги від погроз, що поширювалися на її ім'я іншими через соціальні мережі. До слова, імовірні погрози через соціальні мережі, на які вказувалось у свідченнях, не були розглянуті. Останнє може свідчити про недостатність знань з проявів кібербулінгу, зокрема, під час складання відповідних адміністративних протоколів.

Кібергрумінг у правовому полі. Щодо протидії правопорушенням, пов'язаним з кібергрумінгом, то *національне законодавство безпосередньо не містить положень, спрямованих на реалізацію статті 23 Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства.* Звісно, розслідування цих злочинів можна розглядати через інші статті Кримінального кодексу, а саме: статті 153–159 щодо сексуального насильства, зокрема, стосовно дітей. Гірше, коли йдеться про правопорушення, скоєні онлайн, де можна хіба що застосувати норми статті 301 Кримінального кодексу щодо виготовлення, збуту та розповсюдження порнографії.

Як практичний приклад можна навести провадження Департаменту кіберполіції щодо викриття чоловіка, який у соцмережах примушував дітей до створення порнографічних зображень. «Входячи у довіру до неповнолітніх, зловмисник примушував їх до створення власних фото та відео порнографічного характеру, після чого шантажував оприлюдненням цих фото. Отриману фото- та відеопродукцію зловмисник використовував для власних потреб і для обміну на тематичному російському закритому веб-ресурсі. Наразі зловмиснику вже оголошено про підозру у вчиненні злочину, передбаченого ч. 4 ст. 301 КК України. Наразі йому загрожує до десяти років ув'язнення».

Незважаючи на декларування забезпечення прав та безпеки дітей в інформаційному середовищі в стратегічних документах, їх реального втілення в правовому полі наразі не спостерігається. Закон щодо протидії булінгу виглядає недостатнім для попередження ризиків порушення прав та

насильства стосовно дітей у цифровому середовищі.

3. Міжнародні та регіональні стандарти

Норми міжнародного права в галузі прав людини/дитини, включаючи як стандарти ООН, так і регіональні інструменти з прав людини, повинні становити основу для розробки національного законодавства запобігання та протидії кібербулінгу та кібергрумінгу. У цій частині проаналізовано документи, видані Організацією Об'єднаних Націй та Радою Європи щодо захисту прав дітей в інформаційному просторі.

Глобальний рівень. Конвенція ООН про права дитини (1989) дає найбільш повний виклад прав дітей і водночас наділяє ці права силою міжнародного права**.** У Статті 2 ідеться про те, що держави-учасниці поважають і забезпечують усі права, передбачені цією Конвенцією, за кожною дитиною, яка перебуває в межах їх юрисдикції, без будь-якої дискримінації незалежно від раси, кольору шкіри, статі, мови, релігії, політичних або інших переконань, національного, етнічного або соціального походження, майнового стану, стану здоров'я й народження дитини, її батьків чи законних опікунів або яких-небудь інших обставин.

Статтею 16 міжнародного договору передбачено, що «жодна дитина не може бути об'єктом свавільного або незаконного втручання в здійснення її права на особисте й сімейне життя, недоторканність житла, таємницю кореспонденції або незаконного посягання на її честь і гідність». Стаття 19 гарантує, що держави-учасниці вживають всіх необхідних законодавчих, адміністративних, соціальних і просвітніх заходів для захисту дитини від усіх форм фізичного та психологічного насильства, образи чи зловживань, відсутності піклування чи недбалого й брутального поводження та експлуатації, включаючи сексуальні зловживання, з боку батьків, законних опікунів чи будь-якої іншої особи, яка турбується про дитину. У Статті 39 держави-учасниці вживають всіх необхідних заходів для сприяння фізичному та психологічному відновленню та соціальній інтеграції дитини, яка є жертвою будь-яких видів нехтування, експлуатації чи зловживань, катувань чи будь-яких жорстоких, нелюдських або принижуючих гідність видів поводження, покарання чи збройних конфліктів. Таке відновлення й реінтеграція повинні здійснюватися в умовах, що забезпечують здоров'я, самоповагу й гідність дитини.

У мотивувальній частині Факультативного протоколу до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції та дитячої порнографії висловлено стурбованість щодо використання інтернет-, інших інформаційних

технологій для поширення дитячої порнографії. Від цього часу та впродовж тривалого періоду Комітет ООН з прав дитини (далі Комітет ООН) у своїх коментарях констатує необхідність забезпечення та захисту прав дитини в цифровому середовищі. У 2014 році ним проведено відповідну дискусію щодо цього.

У Загальному коментарі 13 (2011) щодо статті 19 Конвенції Комітет ООН зауважив на психологічному залякуванні, а також приниженні дітей з боку дорослих чи інших людей (кібербулінг), зокрема через використання інформаційно-комунікаційних технологій, таких як мобільні телефони, Інтернет та інше. Саме тому держава має вжити заходів щодо захисту прав дітей, підвищення їх обізнаності використанні інформаційних технологій.

Згодом у Загальному коментарі №20 (2016) про реалізацію прав дитини в підлітковому віці Комітет ООН наголошує на важливості цифрових технологій для обміну інформацією, навчання та вираження поглядів. Цей інститут також привертає увагу до ризиків правам дитини, які несе із собою цифрове середовище. До цих ризиків, зокрема, відносять і кібербулінг та кібергрумінг. Замість обмежувати доступ підлітків до інформаційних технологій Комітет ООН рекомендує: «<…> захищати їх від загроз за допомогою широких стратегій, зокрема підвищення обізнаності щодо мережевих ризиків, а також стратегій, спрямованих на забезпечення їх безпеки, посилення законодавства та правоохоронних механізмів з тим, щоб добиватись вирішення проблем насильства стосовно дітей в Інтернеті та вести боротьбу з безкарністю, а також навчання батьків та фахівців, які працюють з дітьми. Державам наполегливо пропонується забезпечити активне залучення підлітків до вироблення та впровадження ініціатив, спрямованих на посилення безпеки в Інтернеті, зокрема через просвіту з боку однолітків. Потрібні й інвестиції на розвиток технологічних рішень сфери попередження та захисту, а також забезпечення можливості отримання допомоги та підтримки. Державам рекомендовано вимагати від підприємств більшу обережність щодо прав дітей для виявлення, попередження та пом’якшення ризиків правам дитини в час використання ними електронних ЗМІ та інформаційно-комунікаційних технологій.

На час написання огляду Комітет ООН з прав дитини розпочав підготовку Загального коментаря щодо прав дитини у цифровому середовищі. Ціллю майбутнього коментаря повинно стати посилення аргументів активних дій у цій сфері, а також визначити, які заходи слід вжити державам для виконання їх зобов’язань з просування та захисту прав дітей у цифровому середовищі та за його допомогою, а також як співпрацювати в цьому напрямку, скажімо, з бізнесом.

Ризики дотриманню прав дитини в інформаційному просторі стали

предметом уваги й Спеціального представника Генерального секретаря ООН з питань насильства стосовно дітей (далі – Спеціальний представник) у його Доповіді 2016 року, адресованій Раді з прав людини. У Доповіді звертається увага на виклик кібербулінгу, що набирає обертів з розвитком інформаційних технологій та доступом дітей до них. «Кібербулінг – це одна з найбільших проблем стосовно дітей, що пізнають світ мереж. Європейські дослідження свідчать, що поширення образливих повідомлень не найбільший ризик у цифровому середовищі, але такі повідомлення найчастіше тривожать дітей – більшість дітей, які отримували такі повідомлення, зверталися по соціальну підтримку, а 6% видаляли або блокували такі повідомлення».

Для запобігання та протидії кібербулінгу Спеціальний представник пропонує зосередитись на формуванні відповідного законодавства, програм освіти дітей та батьків, підвищенні фахового рівня фахівців, які працюють з дітьми. «Деякі країни прийняли спеціальне законодавство щодо протидії кібербулінгу. Розробляючи законодавство та політики щодо кібербулінгу, слід мати на увазі його неоднаковий вплив на дітей різного віку». У цій же доповіді пропонуються моделі законодавства із захисту прав дітей від кібербулінгу.

1. Держава не ухвалює окремого законодавства з протидії кібербулінгу, якщо наявні норми кримінального законодавства щодо домагань, цькування, розкриття особистої інформації забезпечують достатній захист. Такі норми можуть доповнюватись цивільно-правовими заходами, зокрема, із залученням омбудсмена чи інституту захисту персональних даних.

2. Включення до законодавства правопорушень, пов'язаних із кібербулінгом та кіберграмінгом, зокрема, публікація інтимних фото без згоди, опосередковане домагання та подання себе в Інтернеті як іншої особи.

3. Закон надає можливість особі звертатися до суду за образи через Інтернет, зокрема вимагати відповідних заборонних приписів. Ці приписи можуть включати заборону контактувати з особою, обмеження користування засобами комунікацій або навіть тимчасове чи постійне вилучення засобу комунікації, за допомогою якого здійснювався булінг.

4. Створюється окремий інститут, до повноважень якого належить питання кібербулінгу та інших порушень прав людини через інформаційні технології. Така інституція проводить розслідування за скаргами, формує стандарти безпеки в Інтернеті, взаємодіє з інтернет-посередниками щодо контенту, який може розглядатись як кібербулінг.

5. Законодавство, спрямоване на школи та освіти. Широкі просвітницькі програми спрямовані на надання повної інформації людям щодо можливих засобів захисту, відповідних послуг.

Регіональний рівень. Європейська Конвенція захисту прав людини та основоположних свобод поширюється як на повнолітніх, так і дітей. У

практиці Європейського суду з прав людини наявні справи пов’язані із захистом прав у цифровому середовищі, зокрема K.U. проти Фінляндії, яка стосується крадіжки ідентичності. Від імені дванадцятирічного хлопчика на інтернет-сайті знайомств було розміщено оголошення сексуального характеру. Згідно із чинним тогочасним Фінським законодавством, ані поліція, ані суди не могли вимагати від провайдерів надання інформації стосовно особи, яка розмістила інформацію. Провайдери відмовились давати інформацію про особу, посилаючись на її конфіденційність. ЄСПЛ констатував порушення статті 8 Конвенції, вирішивши, що розміщення оголошення було злочинною дією, оскільки зробило неповнолітнього ціллю педофілів. ЄСПЛ постановив, що ефективне розслідування не могло бути розпочато через наявність обов'язкової умови дотримання конфіденційності. На думку ЄС, «слід було прийняти законодавство, яке могло б узгодити принцип конфіденційності інтернет-послуг з інтересами захисту суспільного порядку, попередження злочинів та захисту прав і свобод інших осіб, зокрема дітей та інших вразливих груп».

Конвенція про захист дітей від сексуальної експлуатації та сексуального насильства (далі – Лансаротська конвенція) була першим міжнародним інструментом, який криміналізує домагання дітей для сексуальних цілей через інформаційні та комунікаційні технології (ІКТ)». Стаття 23 Лансаротської конвенції визначає: «Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації умисної пропозиції, зробленої дорослою людиною за допомогою інформаційно-комунікаційних технологій, зустрітися з дитиною, яка не досягла віку, передбаченого пунктом 2 статті 18 цієї Конвенції, для скоєння проти неї одного з правопорушень, передбачених підпунктом «a» пункту 1 статті 18 або підпунктом «a» пункту 1 статті 20 цієї Конвенції, якщо після цієї пропозиції відбулись істотні дії, що призвели до такої зустрічі». Правопорушення, передбачені підпунктом «a» пункту 1 статті 18, включають: «a) заняття діяльністю сексуального характеру з дитиною, яка не досягла передбаченого законодавством віку для заняття діяльністю сексуального характеру; b) заняття діяльністю сексуального характеру з дитиною, коли: використовується примус, сила чи погрози або насильство здійснюється зі свідомим використанням довіри, авторитету чи впливу на дитину, зокрема в сім’ї, або насильство здійснюється в особливо вразливій для дитини ситуації, зокрема, з причини розумової чи фізичної неспроможності або залежного становища». Правопорушення, передбачені підпунктом «a» пункту 1 статті 20, включають «виготовлення дитячої порнографії».

У 2015 році Комітет учасниць Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства оприлюднив позицію щодо 23 статті Лансаротської конвенції. Зокрема, Лансаротський комітет

звернув увагу, що «15. Стаття 23 Лансаротської конвенції не вимагає фактичного вчинення зазначених вище злочинів, але спрямована на кримінальну відповідальність за підготовку дорослими правопорушень». У зв'язку із цим: «16. Держави можуть розглянути питання посилення законодавства щодо запобігання вчиненню сексуальних злочинів, включаючи онлайн-грумінг проти дітей через інформаційні та комунікаційні технології». Водночас Комітет звертає увагу: «17. Залучення дітей через інформаційні та комунікаційні технології не обов'язково призводить до особистої зустрічі. Вони можуть тривати в мережі, однак завдати шкоди дитині. Сексуальні злочини, які навмисно здійснюються під час онлайн-зустрічі за допомогою комунікаційних технологій, часто пов'язані з виробництвом, володінням і передачею дитячої порнографії».

Лансаротський комітет зауважує, що через стрімкий розвиток технологій та, відповідно, виклики в розслідуванні злочинів, пов'язаних з їх використанням, вимоги статті 23 Конвенції можуть не відповідати ситуації дня сьогоднішнього, тим паче, завтрашнього. «20. Загальне явище онлайн-грумінгу розвивається паралельно з інформаційно-комунікаційними технологіями. Тому його розуміння не повинно обмежуватися часом розроблення Конвенції, у якій зазначено визначення (кібергрумінгу – ред.), але його слід розуміти й діяти відповідно до актуальності сьогоднішнього чи завтрашнього дня. Оскільки статичне визначення онлайн-грумінгу є неможливим, Сторонам слід розглянути можливість поширення криміналізації й на ті випадки, коли сексуальне насильство не є результатом особистої зустрічі, а здійснюється онлайн».

Лансаротський комітет наголошує на тому, що відповідальність за розслідування та переслідування обвинувачених за правопорушення, пов'язані з кібергрумінгом, повинні залишатися виняткова в компетенції правоохоронних органів. Цільові НУО можуть надавати за запитами допомогу, але вони не повинні підміняти собою правоохоронні служби. Водночас він підтверджує необхідність широкого залучення різних стейкхолдерів для запобігання та протидії цьому явищу. «23. Для того, щоб розслідування та кримінальне переслідування онлайн-грумінгу були ефективними, необхідним є забезпечення навчанням та ресурсами для всіх органів, відповідальних за розслідування справ, переслідування злочинців та захист жертв онлайн-грумінгу. 24. Громадянське суспільство також відіграє ключову роль у захисті дітей та молоді, які стали жертвами сексуального насильства та експлуатації. Тому їм також слід виділити адекватні засоби».

Як і інституції ООН, Лансаротський комітет підтверджує нагальну необхідність навчання дітей користуванню інформаційними технологіями та відповідній безпеці. «25. Дітям слід надати можливість користуватися

перевагами інформаційно-комунікаційних технологій. Вони повинні знати про ризики та небезпеки, притаманні цифровому світу, особливо ті, які породжуються надмірною сексуальністю суспільства. Можливості та ризики інформаційних та комунікаційних технологій повинні бути включені до всіх шкільних програм». Позиція Лансаротського комітету змушує констатувати, що Україна вже спізнюється із формуванням політики запобігання та протидії кібергрумінгу.

Права дитини в цифровому середовищі визначено одним з пріоритетів Стратегії Ради Європи з прав дитини (2016–2021). Серед проблем забезпечення прав дитини Стратегією констатовано й ризик насильства стосовно дітей у цифровому середовищі. «Проте цифрове середовище також пропонує дитині шкідливий контент і його наслідки, конфіденційність і питання захисту даних та інші ризики, зокрема сексуальне насильство онлайн і надмірний вплив сексуалізованих зображень. У деяких випадках, таких, як кібербулінг та самовикриття, власна поведінка дітей в Інтернеті може завдати шкоди іншим і становити небезпеку для них. Батьки та вчителі недостатньо докладають зусиль для того, щоб встигати за розвитком технологій, так що розрив між поколіннями стає все очевиднішим».

Одним із наслідків реалізації Стратегії повинна стати зміна законодавства та політик у державах-членах для захисту дітей у цифровому середовищі. Стратегія Ради Європи пропонує й інструмент зменшення наслідків ризиків досягнення пріоритету Стратегії.

Технології розвиваються швидше, ніж стандарти та інструменти Ради Європи – більше інвестицій в ІКТ та дослідження, партнерство з приватним сектором
Стандарти та інструменти Ради Європи не досягають ключових учасників в інтернет-управлінні - мультидисциплінарний підхід, включаючи приватний сектор

Ще одним цінним документом, що визначає стандарти Ради Європи з прав дитини в цифровому середовищі, є Рекомендації CM/Rec (2018)7 Комітету Міністрів державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі, частиною яких є відповідне Керівництво. Відповідно до Рекомендацій, державам пропонується, щоб законодавство щодо прав дітей у цифровому середовищі переглядалось на постійній основі та було за потреби технологічно нейтральним, зважаючи на стрімкий розвиток інформаційних технологій. Законодавство повинно містити всі види правопорушень та різні види відповідальності згідно з міжнародними інструментами Ради Європи. Крім того: «73. Комплексна правова база повинна передбачати превентивні та захисні заходи щодо цифрового середовища;

надавати підтримку батькам і опікунам; забороняти всі форми насильства, експлуатації та зловживання; включати ефективні засоби правового захисту, послуги з відновлення та реінтеграції; встановити консультації для дітей і з питань ґендерної проблематики, механізми фіксування та подання скарг; охоплювати механізми для консультацій та участі дітей; створити механізми підзвітності для боротьби з безкарністю». Рекомендації наполягають на залученні всіх можливих стейкхолдерів, співпрацю з підприємствами, що надають послуги освітнім середовищем.

У 2017 році Європол оприлюднив звіт щодо сексуального примусу та шантажу дітей онлайн. Мета звіту подвійна: підвищити усвідомлення того, що явище сексуального примусу та шантажу дітей онлайн є однією з найнебезпечних загроз для дітей у мережі Інтернет, і зробити внесок у публічне обговорення питань ефективного реагування на нього, особливо, що стосується механізмів повідомлення та підтримки в країнах-членах ЄС. Звіт підтверджує складність розслідування злочинів, пов'язаних з кібергрумінгом. Висновки цього звіту є важливими, зважаючи на необхідність формування національної політики протидії цим правопорушенням. «1. Існують дві основні мотивації для сексуального примусу та шантажу дітей через мережу Інтернет: сексуальна та фінансова. Неповнолітні є жертвами обох цих мотивацій, проте сексуальне задоволення злочинця, очевидно, є основним мотиваційним чинником. Злочини з фінансовою мотивацією скоюють переважно організовані злочинні групи, локалізовані за межами Європейського союзу.
2. Одним із головних чинників, який обмежує сьогодні здатність оцінювати справжню сутність явища сексуального примусу та шантажу дітей онлайн і боротися з ним, є брак спільного розуміння зацікавленими сторонами, такими, як законодавча й судова системи, правоохоронні органи, неурядовий сектор, а також засоби масової інформації. 3. Сексуальний примус та шантаж дітей через мережу Інтернет як новий вид злочину, що з'явився в цифрову еру, є недостатньо дослідженим. Прогалини в дослідженнях обмежують здатність формувати стратегії та програми втручання, що базуються на фактах, – як на рівні виявлення нових випадків, так і розроблення відповідних механізмів повідомлення, законодавчих актів і стратегій для запобігання злочинам та реалізації втручань, які враховують потреби жертви, правопорушника та інших груп зацікавлених осіб. 4. У контексті профілактичного втручання спостерігається брак просвітницьких програм, які пояснюють характеристики сексуального примусу та шантажу дітей онлайн та аналізують основні елементи цього явища. 5. Механізми повідомлення повинні використовувати багатодисциплінарний підхід у формі перехресних повідомлень за участі різних сторін. Відмінності в цілях таких сторін, особливо відсутність зв'язку між механізмами повідомлення та програмами підтримки, ускладнюють

узгодженість і знижують ефективність дій у цій сфері».

На жаль, Україна вже спізнюється з формуванням політики захисту дітей у цифровому середовищі. І якщо протидія кібербулінгу хоча б частково може здійснюватись через заходи, передбачені відповідним Законом, то з кібергрумінгом ситуація виглядає гірше. Водночас наявні пріоритети довгострокових рішень дозволяють працювати над формуванням та реалізацією політики із забезпечення та захисту прав дітей у цифровому середовищі. Крім того, пропоновані інституціями Ради Європи шляхи та способи здійснення цих політик можуть стати дороговказом для вироблення відповідних рішень.