Жовтень 2021

Олексій Волошин,

юрист Лабораторії цифрової безпеки

Як захистити дітей та не заблокувати Інтернет в Україні?

Інтернет є важливим джерелом інформації у житті дітей під час здобуття освіти, соціалізації та самореалізації. Водночас, попри переваги, які використання мережі надає для їх інтелектуального розвитку, Інтернет є достатньо токсичним середовищем. Протиправний та неприйнятний контент широко поширений в Інтернеті та часто загрожує фізичному та психологічному здоров'ю дітей. Держави і технологічні компанії по всьому світу намагаються знайти кращу модель для протидії його поширенню. Видалення очевидно протиправного контенту або обмеження до нього доступу є легітимним інтересом держави, що відповідає обов'язку захищати права інших користувачів. Втім, у пошуках шляхів ефективної протидії таким явищам важливо зберегти баланс між захистом дітей як вразливої категорії населення та свободою вираження поглядів, правом на приватність та правом на доступ до інформації. Цей огляд присвячений тому, як країни шукають цей баланс у сфері протидії контенту, що може зашкодити розвитку дітей, в контексті обмеження доступу до такого контенту чи його блокування, та потенційними рішеннями для України.

Загальні підходи до захисту дітей онлайн в Україні

Донедавна тематика безпеки дітей в Україні не належала до пріоритетних. Більше десяти років тому Україна вперше передбачила кримінальну відповідальність за поширення дитячої порнографії та встановила можливість обмеження доступу до неї у Законі України "Про телекомунікації". Оператори, провайдери телекомунікацій мали зберігати та надавати інформацію про з'єднання свого абонента стосовно таких протиправних діянь.

Вже з 2019 року ці питання набули для уряду більшого значення. Зокрема, парламент ухвалив Закон України №1256-IX, який імплементує в українське законодавство норми Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротська Конвенція). Цим законом Верховна Рада конкретизувала або визначила нові склади злочинів, зокрема

щодо сексуального домагання до дитини; свідомого отримання доступу, придбання, володіння, виготовлення або розповсюдження дитячої порнографії; або проведення видовищного заходу сексуального характеру за участю неповнолітньої особи.

Проєкт Концепції та плану заходів з розвитку цифрових прав дітей від січня 2021 року підтверджує важливість захисту прав дітей для уряду. У ньому використання поширеного раніше поняття “дитяча порнографія” замінили на поняття “сексуальної експлуатації та насильства над дітьми” (СЕНД), що загалом відповідає європейським підходам.

На жаль, Концепцію досі не ухвалили - однак саме на термінологію цього проєкту, а також Закону України “Про електронні комунікації”, Кримінального кодексу та Кодексу України про адміністративні правопорушення, ми спиратимемось при проведенні аналізу.

Проєкт Концепції визначає СЕНД як використання дитини у діяльності порнографічного характеру незалежно від того, чи носить така діяльність добровільний чи примусовий характер. Актуальними нормами законодавства, які спрямовані на протидію цьому контенту є статті 155, 156-1, 301-1 та 302-2 Кримінального кодексу, які впроваджено із вищезгаданим Законом №1256-IX.

Кримінальний кодекс визначає, що дитяча порнографія - це зображення у будь-який спосіб дитини чи особи, яка виглядає як дитина, у реальному чи змодельованому відверто сексуальному образі або задіяної у реальній чи змодельованій відверто сексуальній поведінці, або будь-яке зображення статевих органів дитини в сексуальних цілях. Як вже згадувалося вище, обмеження доступу до такого контенту передбачає Закон України “Про телекомунікації” та його наступник - Закон України “Про електронні комунікації”. Обмежують доступ провайдери доступу до Інтернету за рішення суду - втім, механіку втілення цього заходу в життя законодавство не передбачає.

Серед іншого шкідливого для дітей контенту, який згадує Концепція, виділимо **кібербулінг** - знущання, приниження, агресивні напади, які здійснюються за допомогою різних гаджетів (зокрема телефонів), з використанням Інтернету, будь-яких електронних (цифрових) технологій. Хоча станом на сьогодні кібербулінг є адміністративним правопорушенням, механізмів обмеження доступу до такого контенту не передбачено.

У Концепції згадується також інший контент, поширення якого може становити ризик для дітей:

- домагання у сексуальних цілях або для цілей торгівлі людьми;
- принизливе стереотипне зображення та надмірна сексуалізація дітей;
- заклики до насильства та нанесення собі пошкоджень;
- непридатний для дитини рекламний контент;

- контент, що принижує людську гідність, містить мову ворожнечі та заклики до дискримінації.

Обмеження доступу до цих типів контенту законодавство теж напряму не передбачає. Проєкт концепції декларує прагнення уряду розробити правовий режим обмеження доступу до матеріалів, що містять СЕНД, і у наступних частинах огляду головний фокус буде саме на обмеженні доступу до цього виду протиправного контенту.

Основні методи обмеження доступу до шкідливого контенту

Обмеження доступу до будь-якого контенту за своєю суттю є втручанням у свободу вираження поглядів, як користувачів, так і Інтернет-платформ. З огляду на це, відповідні обмеження мають відповідати міжнародним стандартам захисту прав людини. Відповідно до статті 19 Міжнародного пакту про громадянські та політичні права та статті 10 Європейської конвенції про права людини, будь-які обмежувальні заходи мають бути:

- передбачені законом;
- переслідувати легітимну мету;
- бути необхідними у демократичному суспільстві.

Будь-який захід із обмеження доступу до сайту повинен бути частиною чіткої правової рамки, яка б забезпечувала контроль щодо обсягу обмеження та ефективний контроль для попередження зловживань, особливо для попередження блокування правомірного контенту та боротьби із дублюванням шкідливої інформації. Також важливо розрізняти блокування шкідливої інформації та всього веб-сайту, адже останній може містити як правомірну, так і протиправну інформацію, а тому підхід до обмеження доступу має враховувати і цей фактор.

При визначенні способу обмеження доступу до сайту слід враховувати (1) пропорційність, що включає прагнення не обмежувати легальний контент; (2) обрання найдоречнішого посередника; (3) вплив на роботу мережі; (4) вартість блокування; (5) легкість обходу обмеження.

Найефективнішим заходом є цілковите видалення протиправного контенту на ресурсах хостинг-провайдера. Інші способи лише обмежують доступ до контенту та залишають можливість за допомогою технічних заходів обійти заборону. Серед цих способів можна виділити:

- зобов'язання доменного реєстратора з блокування DNS: локальному DNS-серверу провайдера наказується повертати хибні результати щодо заблокованого матеріалу. Замість повернення правильної IP-адреси, що відповідає доменному імені, DNS-сервер провайдера поверне код помилки "не існує" або перенаправить користувачів на вказану веб-сторінку, яка пояснює, що запит заблоковано. Користувачі можуть легко змінити свої DNS-сервери, щоб уникнути блокування або отримати доступ

до матеріалів, ввівши IP-адреси безпосередньо до браузера. Цей метод блокування зазвичай поєднується з DPI і широко застосовується в Китаї та на Близькому Сході);

- зобов'язання провайдера доступу до Інтернету -
    - блокувати за IP-адресою - як правило всім пристроям присвоюється IP-адреса, яка однозначно ідентифікує їх на інших комп'ютерах, подібно до поштової адреси або поштового індексу;
    - блокувати URL-адресу - найбільш точна ідентифікація ресурсу сайту, який може бути як певною сторінкою нижчого рівня, зображенням чи іншим файлом. Фільтрація URL-адрес вимагає від провайдерів не обслуговувати запити щодо певної URL-адреси;
    - використати DPI (глибокий аналіз пакетів) - провайдер доступу до Інтернету здійснює моніторинг трафіку за допомогою DPI-обладнання і може заблокувати доступ кінцевого користувача до визначеної веб-сторінки. Застосування DPI може бути трьох типів: 1) мінімальний аналіз; 2) зведений аналіз; 3) докладний, інвазивний аналіз вмісту пакетів даних;
- Поєднання кількох вищезгаданих способів.

Блокування IP-адрес зазвичай реалізується в поєднанні з іншим заходом (наприклад, фільтрація DPI або URL-адрес) з метою зменшення ризику помилкового спрацьовування. Блокування IP-адреси може бути доцільним у випадку, коли протиправний контент розміщується на окремому сервері, що робить ризик блокування правомірного контенту меншим. Однак у більшості випадків блокування IP-адреси все ж є недостатньо точним.

Блокування DNS та URL-адрес покриває лише трафік за протоколом передачі гіпертексту ("HTTP"). Фільтрування трафіку за протоколом HTTPS суттєво складніше та можливе за допомогою проксі-сервера, який виконує атаку, використовуючи надійний криптографічний сертифікат, щоб розшифрувати, перевірити та повторно зашифрувати запити, перш ніж переслати чи заблокувати їх.

Застосування DPI-блокування визначених веб-сторінок в Європі є ускладненим, оскільки межує із «загальним моніторингом», який заборонено статтею 15 Директиви 2000/31/ЄС про електронну комерцію. Крім того, при використанні цього способу блокування необхідність захоплення, аналізу та збирання потоків трафіку може значно погіршити продуктивність мережі.

На практиці ж, мета блокування - якнайбільше обмеження або ускладнення доступу на території України. Повне видалення протиправних матеріалів матиме перевагу перед обмеженням доступу до них. Якщо сервери із протиправною інформацією розташовано в Україні, то основні дії мають бути спрямовані на її видалення – через власників сайтів та хостинг-провайдерів,

можливо – з залученням правоохоронних органів. Втім, блокування стає чи не єдиним доступним заходом, якщо сервери з інформацією, що порушує законодавство, розташовані поза межами України. Такий обов'язок може покладатися на провайдера доступу до Інтернету.

Блокування має низку недоліків, серед яких відносна легкість обходу обмежень (наприклад, за допомогою VPN, просте введення IP-адреси для обмежень за DNS, "дзеркал" проксі-серверів, Smart DNS, SSH тунель, зміна протоколу чи сервіс скорочення посилань для блокувань за URL-адресами, TOR тощо). При цьому при обранні деяких методів блокування може обмежуватись доступ до правомірних сайтів.

Проаналізувавши міжнародні стандарти у сфері захисту свободи вираження поглядів та технічну складову обмеження доступу до протиправного контенту, ми пропонуємо сконцентруватися на досвіді інших країн щодо питання обмеження доступу до сайтів, на яких розміщується шкідливий для дітей контент.

Європейський Союз

Основним профільним документом у ЄС, який передбачає норми для боротьби із СЕНД, є Директива ЄС 2011/93/ЄС щодо протидії сексуальному насильству та сексуальній експлуатації дітей та дитячій порнографії. Стаття 25 Директиви напряму передбачає обмеження доступу до СЕНД у країнах ЄС, а у 2016 році Європейська Комісія оцінювала впровадження цієї Директиви загалом та її статті 25 окремо.

Згадана норма передбачає обов'язок держав-членів ЄС негайно видаляти матеріали на сайтах, доступ до яких надається з їх території та докладати зусиль для видалення або обмеження доступу до матеріалів, доступ до яких надається з третіх країн. Блокування має здійснюватись за прозорими процедурами, бути необхідним і пропорційним, відповідальні органи мають інформувати користувачів щодо причин обмежень доступу до сайтів, забезпечується можливість судового оскарження заходів.

Подібні запобіжники найчастіше потрібні для уникнення блокування правомірного контенту, позаяк деякі методи блокування найчастіше мають такий побічний ефект. Європейська Комісія у коментарі до Директиви пояснює, що загалом вітаються будь-які заходи, які досягають мети блокування цього контенту, включаючи добровільний моніторинг та блокування Інтернет-посередниками.

Держави-члени ЄС часто впроваджують Директиву через закріплення відповідних норм у кримінально-процесуальному законодавстві (вилучення матеріалів у кримінальному процесі чи прямий припис про оперативне видалення протиправних матеріалів), та через Директиву ЄС про електронну комерцію. Імплементація зобов'язання через Директиву про електронну комерцію передбачає обмеження відповідальності Інтернет-посередників, якщо вони виконують нейтральну роль при передачі чи збереженні інформації (ніяким

чином її не модерують) та у разі, якщо вони дізнаються про наявність протиправного контенту у своїх мережах, то вони оперативно обмежують доступ до нього. Це положення є основою для розвитку у країнах ЄС процедури notice and takedown.

Держави-члени впровадили процедури notice and takedown щодо контенту, який містить СЕНД, через національні гарячі лінії за допомогою яких користувачі можуть повідомити про відповідні матеріали. Мережею таких гарячих ліній є INHOPE: вона включає 46 гарячих ліній у 42 країнах, включно зі всіма державами-членами ЄС.

Гарячі лінії зазвичай спочатку отримують повідомлення від користувачів про місцезнаходження протиправного контенту (URL-адреса), потім проводять аналіз контенту та у випадку його суперечності закону інформують хостинг-провайдера та правоохоронні органи. Щодо видалення контенту, то часто воно можливе без залучення правоохоронних органів, залежно від домовленості між операторами гарячих ліній, правоохоронними органами та провайдерами (наприклад, у Франції, Угорщині, Польщі, Португалії, Великій Британії тощо). У деяких країнах правоохоронні органи інформують провайдерів про необхідність видалення протиправного контенту (зокрема у Німеччині, Болгарії, Естонії, Фінляндії, Словаччині), а у деяких - необхідне рішення суду з можливістю, щоправда, тимчасово блокувати контент до винесення відповідного рішення (Кіпр та Хорватія).

Якщо контент, що містить СЕНД, знаходиться у юрисдикції третьої країни, то держави-члени ЄС використовують ресурси мережі INHOPE для його видалення, у інших випадках, гарячі лінії спрямовують звернення до відповідальних правоохоронних органів у цих країнах (часто через Європол чи Інтерпол). За даними Єврокомісії, взаємодія через гарячі лінії показує значну ефективність у швидкості видалення протиправного контенту.

У випадках, коли видалення контенту з різних причин є неможливим, держави-члени ЄС також використовують механізми блокування, які у деяких країнах потребують дозволу суду (Іспанія, Угорщина), запитів правоохоронних органів (Франція, Італія, Португалія) або ж впроваджуються провайдерами добровільно (Болгарія, Чехія, Велика Британія). Здебільшого правоохоронні органи або галузеві регулятори формують список протиправних веб-сторінок та передають його провайдерам. Деякі країни (Франція, Італія) передбачають більш детальний процес обмеження доступу до протиправного контенту.

Наприклад, грецький телеком-регулятор сповіщає провайдерів про інформацію, яка повинна бути заблокована та яке повідомлення має відображатись для користувачів. Власник веб-сторінки може оскаржити блокування протягом двох місяців. У Фінляндії поліція має право створити та підтримувати список сайтів, які містять СЕНД, та інформувати провайдерів щодо повідомлення, яке має відображатись користувачам, які прагнуть отримати доступ до сайту. Оскаржити рішення поліції можливо у судовому порядку.

Окремо варто згадати про Директиву про аудіовізуальні медіапослуги, яка вимагає від платформ спільного доступу до відео, таких як YouTube, вживати належних заходів для захисту неповнолітніх від контенту, який може зашкодити їх фізичному, розумовому чи моральному розвитку, а також широкої громадськості від контенту, що стосується сексуального насильства над дітьми.

11 лютого 2021 року Європейська Комісія розпочала громадські консультації щодо своєї ініціативи боротьби з СЕНД в Інтернеті, мета якої - покладання на Інтернет-посередників зобов'язання виявляти СЕНД та повідомляти про це відповідним органам влади. Ініціатива, яку Комісія вперше окреслила у своїй стратегії щодо більш ефективної боротьби з сексуальним насильством над дітьми у липні 2020 року, передбачає запровадження для постачальників послуг обов'язків виявлення контенту, що містить СЕНД, звітування про нього, та створення Європейського центру запобігання та протидії сексуальному насильству над дітьми для координації та уникнення дублювання зусиль держав-членів. Відповідні пропозиції мали бути опубліковані у другому кварталі 2021 року.

Крім того, наприкінці квітня 2021 року європейські законотворці надали можливість низці Інтернет-посередників (до числа таких компаній належатимуть Facebook та Microsoft) моніторити, видаляти та повідомляти правоохоронним органам про контент, що містить СЕНД. Моніторинг буде здійснюватись щодо відомих матеріалів, що містять СЕНД, із застосуванням хешування. Такий крок з регулювання має наслідком суттєве втручання у право на приватність, що межує з забороненим в рамках ЄС загальним моніторингом, хоча декларується як тимчасовий захід до прийняття нової законодавчої рамки.

Серед інших законодавчих ініціатив, що вплинуть на захист дітей онлайн, є проєкт акта про цифрові послуги (Digital Services Act). Загалом він віддзеркалюватиме норми щодо протиправного контенту, які вже наявні у окремих юрисдикціях (зокрема положення про "терористичний" контент, чи такий, що містить СЕНД). Він передбачає впровадження вимоги видалення протиправного контенту при поясненні відповідних обмежень користувачам, порядок вирішення спорів (включаючи позасудовий) та звітування щодо заходів, спрямованих на обмеження доступу до відповідного контенту.

Іншими гарантіями мають стати врахування принципу необхідності при блокуванні, обмеження блокування у часі, обрання найдоцільнішого посередника (провайдер доступу, хостингу чи доменний реєстратор) для уникнення блокування правомірної інформації. Втім, в окремих випадках оповіщення власника сторінки/контенту не є доречним, особливо якщо існує необхідність попередження кримінальних правопорушень та притягнення до відповідальності за СЕНД.

Сполучене Королівство

Згідно з Sexual Offences Act 2003 року, що діє у Англії та Уельсі, забороняється скачування, виробництво, володіння, розповсюдження, опублікування і реклама непристойних зображень або псевдозображень (включаючи відео) із зображенням дитини до 18 років. Ці дії караються ув'язненням на термін до 10 років.

Серед інших актів, що мають на меті захист дітей онлайн - Digital Economy Act 2017 року, згідно з яким вимагається забезпечення обмеження доступності комерційних порнографічних матеріалів для осіб молодше 18 років. Втім, його положення не були втілені у життя через технічні складнощі та потенційні обмеження права на приватність. Найбільш свіжою ініціативою уряду є проєкт акта під назвою Online Safety Bill. Акт може надати державному секретарю (очільник профільного департаменту цифрової економіки, культури, медіа та спорту) та регулятору (Офіс з питань комунікацій) повноваження щодо регулювання контенту онлайн. Уряд пропонує накласти на пошукових операторів та інших посередників обов'язок проявляти обережність та видаляти шкідливий контент. Регулятор отримає право блокувати доступ до протиправного та шкідливого контенту. Визначення того, що є шкідливим контентом, делегується державному секретареві.

Посередники будуть зобов'язані здійснювати оцінку ризиків стосовно потенційної шкоди від їх платформ. Регулятор розроблятиме профілі ризиків, які мають враховуватися компаніями. При оцінці ризиків компанії матимуть враховувати наскільки швидко розповсюджується протиправний контент, наскільки серйозна шкода, яку контент може завдати. Зокрема, законопроєкт визначає пріоритетним контент, що вважається "терористичним" та котрий містить СЕНД, а також інший "пріоритетний протиправний контент", який буде визначений у нормативних актах державним секретарем.

Компанії будуть зобов'язані мінімізувати наявність "пріоритетного протиправного контенту" на платформі, час його доступності для користувачів, міру його розповсюдження. Крім того, служби підтримки компаній будуть зобов'язані «оперативно» реагувати на скарги щодо протиправного контенту. Подібні зобов'язання пропонуються для обмеження поширення контенту, шкідливого для дітей. Також вводиться окрема категорія оцінки ризиків стосовно шкідливого впливу на дітей, за якою компанії повинні оцінювати ймовірність та серйозність впливу шкідливого контенту на їх платформах.

Проєкт акта вводить суттєві штрафи для порушників - до 18 мільйонів фунтів або 10% світового доходу. Проєкт значно критикується за складність, введення категорії правомірного, але шкідливого контенту, значні повноваження регулятора щодо обмеження свободи слова (повноваження блокування та накладення штрафів). Палата лордів розпочала оцінку акта, яка триватиме щонайменше до кінця грудня 2021 року, та вже виражає занепокоєння щодо

деяких категорій “шкідливого” контенту та розміру штрафів, що на їх думку може призвести до небажаних наслідків (як при впровадженні німецького NetzDG).

Обмеження обігу контенту, що містить СЕНД, в країні здійснюється за допомогою прямого видалення тих матеріалів, які зберігаються на британських серверах, та блокування доступу до списку протиправних сайтів (фільтрація URL-адрес), у формуванні якого беруть участь провідні Інтернет-провайдери, оператори мобільного зв’язку, правоохоронні органи і громадянське суспільство. Таке добровільне обмеження доступу до протиправного контенту здійснюється через Internet Watch Foundation (IWF). Ця організація є національною “гарячою лінією” з моніторингу нелегального Інтернет-контенту, яка стала результатом домовленості уряду, Інтернет-провайдерів та організацій громадянського суспільства і діє як незалежна, саморегульована організація для операцій notice and takedown щодо контенту, що містить СЕНД. Вона приймає повідомлення про протиправний контент і формує “чорний список сайтів”, направляє його Інтернет-провайдерам (близько 60 у країні), операторам мобільного зв’язку та виробникам програмного забезпечення для фільтрування. Саме ці посередники, в свою чергу, інформують спеціальні підрозділи поліції, зокрема National Crime Squad.

Хоча систему критикували за відсутність процедурної прозорості та легку можливість обходу обмежень, виявляється, що системи фільтрації URL-адрес нового покоління можуть запропонувати більшу ефективність без багатьох недоліків інших форм фільтрації. Серед інших інструментів платформи, які варто відзначити, є наявність процедур апеляції проти неточних оцінок IWF, наявність хеш-бази для блокування контенту, який повторно з’являється в мережі (розроблено у співпраці із Microsoft).

Отже, основний тягар обмеження доступу до контенту, що містить СЕНД, покладається на приватний сектор через IWF. Якщо буде прийнято новий закон про безпеку в Інтернеті, то можливим буде значне посилення ролі регулятора у питаннях захисту дітей онлайн.

Австралія

У Австралії є два основних законодавчих джерела заборони контенту шкідливого для дітей - Broadcasting Services Act 1992 року та Кримінальний кодекс. До забороненого контенту належать зображення та відео сексуального насильства над дітьми.

Можна впевнено вважати Комісара з онлайн безпеки першим регулятором у цій сфері. Його було створено у 2015 році на основі Online Safety Act. Регулятор здійснює загальний нагляд за безпекою дітей у цифровому середовищі, адмініструє систему скарг на протиправний та шкідливий контент, може видавати приписи щодо видалення контенту та карати за недотримання законодавства. Він займає центральну позицію у питанні видалення та обмеження доступу до контенту, що містить СЕНД. Комісар сповіщає поліцію про відповідні матеріали та після забезпечення розслідування видає припис хостинг-провайдеру щодо

видалення контенту. Такий припис має розглядатися протягом 24 годин. Недотримання вимог Комісара має наслідком значні штрафи (111000 австралійських доларів для осіб та 555000 австралійських доларів для компаній).

Комісар також є активним членом мережі гарячих ліній INHOPE - при виявлені контенту, який розміщено на серверах держави-члена мережі, її правоохоронні органи будуть швидко оповіщені. За практикою Комісара контент, який комунікується у мережі гарячих ліній, видаляється протягом трьох робочих днів. Якщо контент розміщено на серверах країни поза мережею гарячих ліній INHOPE, то питання вирішується на рівні австралійської поліції механізмами угод про взаємодопомогу у цивільних і кримінальних справах. Комісар та Інтернет-провайдери також мають налагоджену процедуру реагування на кризові онлайн пригоди (прикладом такої пригоди є атака у місті Крайстчерч), що передбачає попередження вірусного розповсюдження матеріалів, які провокують насилля чи підбурюють або вказують на терористичні акти.

Щодо статистики діяльності регулятора, то у 2019-2020 Комісар заборонив доступ до понад 13 000 URL-адрес, 99 відсотків з яких містили контент, що можна кваліфікувати як СЕНД.

У червні 2021 року парламент Австралії прийняв новий Online Safety Act 2021. Цей закон має на меті покращити безпеку в Інтернеті, наприклад, запровадивши захист від кібербулінгу та експлуатації дітей. Він також розширить можливості федерального уряду блокувати та вимагати видалення певного контенту в Інтернеті. Таким контентом є матеріали про кібербулінг, інтимні зображення, поширені без згоди, та навіть питання цькування дорослих австралійців.

Відповідно до закону, користувачі можуть подавати Комісару офіційні скарги щодо контенту онлайн; тоді Комісар буде уповноважений проводити розслідування цих скарг та видавати приписи про видалення. Саме цей закон передбачає видалення контенту протягом 24 годин після отримання повідомлення на відміну від 48 годин у минулій редакції закону.

Закон встановлює дворівневу схему вилучення матеріалів кібербулінгу з соціальних мереж. Два рівні схеми підлягають різним рівням регуляторного нагляду; так, в Австралії існуватимуть:

- платформи, які беруть участь у схемі на добровільній основі;
- платформи, які оголошуються Міністром комунікацій такими, що належать до другого рівня регулювання - підлягають обов'язковим до виконання приписам та штрафам за їх невиконання.

Добровільний режим може обрати будь-яка платформа, яка відповідає базовим вимогам - платформи мають передбачити у своїх правилах користування заборону кібербулінгу, впровадити систему скарг для протидії кібербулінгу, визначити контактну особу для взаємодії з Офісом Комісара. Якщо компанії у рамках цього режиму протягом року не видаляють шкідливий контент та ігнорують приписи Комісара, то їх можуть позбавити цього статусу та порадити їм перейти до другого режиму. Серед відомих сервісів до цього режиму добровільно приєднались TikTok, Twitter, Snapchat, Flickr, WeChat.

До другого режиму належать або ті компанії, які не задовольняють базові вимоги, або великі соціальні мережі, зокрема Facebook, Instagram та YouTube. Практично компанії в рамках цього режиму несуть більшу відповідальність у вигляді значних штрафів через невиконання приписів Комісара. Компанії можуть звернутись до адміністративного суду для оскарження будь-яких рішень про переведення компаній між режимами, накладення штрафів або інші приписи.

Отже, Австралія забезпечує надзвичайно широке та детальне регулювання, дотримуючись принципу “безпека за замовчуванням”, визначаючи спеціальний відповідальний орган та наділяючи його значними повноваженнями щодо обмеження поширення контенту, який є протиправним чи шкідливим.

Ірландія

Ірландія прагне запровадити регулювання подібне до австралійського та британського Online Harms Bill. Опублікований проєкт акта Online Safety and Media Regulation Bill передбачає створення інституту Уповноваженого з онлайн безпеки, який впроваджуватиме обов’язкові кодекси онлайн безпеки та слідкуватиме за їх дотриманням, включно з механізмами обов’язкових приписів та санкцій. У кодексах онлайн безпеки визначатимуться підходи до протидії шкідливому контенту, включаючи такий, що шкодить дітям, процедури notice and takedown. Очікується, що до сфери відповідальності ірландського комісара належатиме не лише протидія поширенню протиправного контенту, але й шкідливого, наприклад кібербулінгу.

Бразилія

У 2014 році Бразилія прийняла Білль про права у Інтернеті. Постачальники Інтернет-застосунків - включають як веб-сайти, так і мобільні застосунки - за його положеннями не несуть цивільно-правової відповідальності за контент, створений користувачами, доки суд не ухвалить рішення про його видалення.

Закон про дітей та підлітків передбачає кримінальну відповідальність за пропозицію, торгівлю, надання доступу, розповсюдження або публікацію будь-якими засобами фотографій, відеозаписів або будь-яких інших записів сексуального характеру за участю дітей чи підлітків. Злочин карається позбавленням волі, яке може бути застосовано до кожного, хто надає засоби або послуги для доступу до такого типу контенту. Це положення застосовується лише тоді, коли постачальник послуг, отримавши повідомлення, не обмежує доступ до

контенту, що порушує права. На практиці це означає, що постачальники послуг повинні реагувати на повідомлення про видалення, щоб уникнути кримінальної відповідальності.

США

Загалом, уряд США не змушує Інтернет-провайдерів або хостинг-провайдерів блокувати або фільтрувати онлайн-матеріали, які захищаються відповідно до міжнародно-правових норм захисту прав людини. У США провайдери ризикують бути притягненими до кримінальної відповідальності за те, що після того, як їм стало відомо про контент, що містить СЕНД, його не вдалося видалити. Розділ 230 Communications Decency Act є основним правилом, яке захищає свободу слова в Інтернеті. Це правило обмежує відповідальність Інтернет-посередників за нейтральну передачу чи зберігання потенційно протиправного контенту.

Незважаючи на серйозну юридичну та культурну підтримку свободи слова в США, обсяг застосування Розділу 230 жорстко критикується. Занепокоєння щодо СЕНД, наклепу, кібербулінгу та кіберзлочинності, терористичного контенту та захисту дітей від шкідливих чи непристойних матеріалів - все це сприяє прагненню реформувати правовий імунітет платформ щодо контенту створеного користувачами.

У своїй первісній формі Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT), який був внесений у Сенат у 2020 році, а також його супровідний законопроєкт у Палаті представників, прагнув покласти на посередників обов'язок моніторингу власних платформ на предмет наявності контенту, що містить СЕНД, для уникнення відповідальності. Крім того, на посередників також міг би покладатись обов'язок використовувати рекомендовані урядом технології для пошуку, повідомлення та видалення контенту, що містить СЕНД, що відкривало б шлях до послаблення шифрування.

Хоча до проєкту було внесено зміни, щоб виключити питання шифрування з реформ Розділу 230, адвокати та деякі вчені-юристи все ж стверджували, що він може створити основу для обмежень шифрування. У травні 2020 року у відповідь на недоліки проєкту Закону, група сенаторів-демократів представила Invest in Child Safety Act 2020 - альтернативний законопроєкт, який би підтримував існуючі стандарти шифрування, а також вирішував питання експлуатації дітей в Інтернеті шляхом посилення фінансової підтримки існуючих механізмів. На жовтень 2021 року актуальним залишається лише Invest in Child Safety Act - він був знову внесений у квітні 2021 року.

Насамкінець, National Center for Missing and Exploited Children - приватна неприбуткова та уповноважена Конгресом ініціатива для протидії поширенню контенту, що містить СЕНД, співпраці з правоохоронними органами та захисту жертв СЕНД. Крім приватних пожертв, організація значно фінансується Департаментом юстиції США. Вона також служить як американська національна

гаряча лінія, член мережі INHOPE. Практично, центр виконує роль аналогічну до британського IWF у питанні протидії поширенню контенту, що містить СЕНД, - отримує повідомлення від громадян, опрацьовує їх, потенційно протиправні матеріали передаються правоохоронним органам та провайдерам. У 2019 році центр отримав майже 17 мільйонів повідомлень із 69 мільйонами одиниць матеріалів, що містять СЕНД, багато з них від таких платформ як Google чи Facebook. Для протидії поширенню такої кількості протиправного контенту центр та компанії задіюють автоматизовані рішення.

Канада

Уряд, як правило, не блокує та не фільтрує контент і не вимагає цього від постачальників послуг. Проєкт Cleanfeed Canada, ініціатива подібна до британського IWF, дозволяє Інтернет-провайдерам блокувати зображення сексуального насильства над дітьми, розміщені за межами Канади (на відміну від вмісту, розміщеного в Канаді, який підлягає видаленню).

У липні 2021 року уряд опублікував технічний документ щодо майбутнього законодавства про шкідливий Інтернет-контент. Запропонований документ пропонує впровадження режиму скарг та видалення для постачальників електронних комунікаційних послуг, що передбачатиме обмеження поширення контенту, що містить СЕНД, пропаганду тероризму, насильства, мову ворожнечі та інтимні зображення, поширені без дозволу. Реагування на скаргу щодо протиправного контенту має здійснюватись протягом 24 годин. Автори проєкту також пропонують уповноважити Інтернет-провайдерів блокувати сайти, які не вилучили протиправні матеріали, та зберігати дані про осіб, які поширюють шкідливий контент та можуть бути зобов'язані відправити цю інформацію правоохоронним органам.

Німеччина

Відповідно до Закону про обмежений доступ до дитячої порнографії в мережах зв'язку 2009 року тамтешні провайдери були зобов'язані блокувати доступ до списку URL-адрес, наданих Федеральним агентством з розслідування кримінальних справ. Закон викликав серйозну критику, оскільки він розглядався як привід для введення інших форм цензури. Після набрання чинності Законом громадськість закликала його негайно скасувати у петиції, яка зібрала понад 130000 підписів, і його було оскаржено у Конституційному Суді. Після зміни уряду Бундестаг скасував цей закон у грудні 2011 року.

Найбільш помітним останнім регулюванням у Німеччині є Network Enforcement Act 2017 року (NetzDG), який вимагає, щоб усі соціальні мережі з принаймні двома мільйонами зареєстрованими користувачами у Німеччині видаляли очевидно протиправний контент протягом двадцяти чотирьох годин після отримання сповіщення. До очевидно протиправного контенту NetzDG відносить Секції 184b та d Кримінального кодексу - поширення дитячої порнографії. Компанії, що володіють соціальними мережами, зобов'язані

подавати звіти кожні шість місяців. За невиконання норм закону передбачені суттєві штрафи (до 5 мільйонів євро штраф, який може збільшитись у десять разів).

У Німеччині є своє гаряча лінія, jugendschutz.net, яка заснована німецькими федеральними землями представленими органами з питань молоді на основі Міжземельної угоди щодо захисту дітей. Ця гаряча лінія фінансується державою на рівні земель та повинна бути професійно та бюджетно незалежною. Jugendschutz.net співпрацює з федеральною поліцією та іншими гарячими лініями у мережі INHOPE для видалення матеріалів СЕНД.

Італія

Італія із ратифікацією Ланцаротської конвенції прийняла низку змін до законів для її впровадження. Вона криміналізувала володіння, розповсюдження матеріалів СЕНД, а також грумінг. Окремі зміни стосувались Інтернет-провайдерів - вони зобов'язані повідомляти про будь-яку компанію чи особу, які розповсюджують матеріали СЕНД, до Національного центру боротьби з дитячою порнографією в Інтернеті, який є частиною поліції, та блокувати такий контент. Невиконання вимог щодо звітування чи видалення матеріалів СЕНД може призвести до накладення значних штрафів.

Національний центр надає Інтернет-провайдерам список сайтів, що містять протиправні матеріали і провайдери забороняють доступ до них. На сайтах, доступ до яких заблоковано, відображатиметься «стоп-сторінка» із зазначенням причин блокування.

Якщо сервер, на якому розміщено протиправний контент, знаходиться в Італії, відповідальні органи проводять видалення протиправний об'єктів, та вживають відповідних заходів для запобігання повторного завантаження. Блокування є єдиною доступною альтернативою, якщо сервер розташований за межами Італії. За необхідності, Регулятор телекомунікацій зобов'язаний перелічити додаткові веб-сайти, на які має бути розповсюджений порядок блокування. На практиці Регулятор часто приписував блокування за IP-адресою або на рівні домену.

Італія має дві гарячі лінії INHOPE, але чинне законодавство не дозволяє їм перевіряти зміст звітів, отриманих від користувачів чи інших гарячих ліній. Тому вони просто надсилають звіти до правоохоронних органів (а саме до Національного центру боротьби з дитячою порнографією в Інтернеті), не перевіряючи зміст.

В Італії також прийнято закон щодо булінгу в школах, у якому визначено кібербулінг. За цим актом Інтернет-провайдери зобов'язані видаляти шкідливий контент на запит законних представників дітей.

Франція

15 лютого 2011 року був прийнятий Закон LOPSI-2, “Закон, спрямований на забезпечення внутрішньої безпеки країни”. Закон передбачає здійснення обов’язкової фільтрації Інтернету для припинення поширення контенту, що містить СЕНД, на підставі складених МВС Франції спільно з громадськими організаціями “чорних списків”, а також негайного блокування ресурсів, що містять протиправний контент за поданням МВС Франції у вигляді наказу (без винесення судового рішення).

Окремим указом Президента Франції, ухваленим у 2015 році, визначено адміністративні заходи щодо блокування веб-сайтів, що містять матеріали, що розпалюють чи виправдовують тероризм, а також сайтів, які демонструють СЕНД. Відповідальний підрозділ боротьби із кіберзлочинами періодично оновлює список сайтів, що підлягають блокуванням. Провайдери мають можливість самостійно обрати технологію блокування.

Згідно із даними національного органу з питань приватності, у 2020 році Центральне управління з питань боротьби зі злочинністю, пов’язаною з інформаційно-комунікаційними технологіями видало 50,448 запитів про видалення контенту (порівняно із 11,874 запитами за рік до цього) та 4,138 запити про деіндексацію (порівняно із 5,883 за рік до цього). Задоволено було 36,710 запитів (73% від загального обсягу), серед них 13,079 запитів стосувалось контенту, що містить СЕНД. При спробі зайти на заблоковані ресурси користувачі потрапляють на сторінку МВС Франції, де зазначаються причини блокування та доступні заходи оскарження через адміністративні суди. Центральне управління кожні чотири місяці переглядає список заблокованих ресурсів на предмет того, чи продовжують вони порушувати місцеві закони.

У травні 2020 року парламент ухвалив закон проти контенту, що сприяє ненависті в Інтернеті, відомий як закон «Авіа». Закон вимагав, щоб основні онлайн-платформи розглядали можливість видалення контенту, який повідомляється користувачами як “протиправний”, протягом 24 годин. Законопроєкт також вимагав, щоб усі сайти видаляли терористичний контент чи такий, що містить СЕНД, протягом однієї години після повідомлення від Центрального управління з питань боротьби зі злочинністю, пов’язаною з інформаційно-комунікаційними технологіями. У разі ігнорування вимог платформи можуть бути оштрафовані на суму до 20 мільйонів євро або до 4 відсотків світового доходу в особливих випадках.

Вимоги закону були суттєво переглянуті Конституційною Радою у червні 2020 року після апеляції групи сенаторів. Рада встановила, що більшість положень закону, зокрема зобов’язання щодо вилучення контенту у встановлений термін, порушують свободу вираження поглядів. Таким чином, Франція практично буде синхронізувати власні нові ініціативи у цій сфері із прийняттям в ЄС нових рамкових актів, а саме Digital Services Act.

Насамкінець, у Франції було запроваджено спеціальний закон про захист неповнолітніх щодо цифрових медіа-послуг на замовлення для імплементації Директиви про аудіовізуальні медіа-послуги. Цей закон вимагає класифікації програм, перевірки віку та заборони трансляції контенту, який може завдати шкоди дітям.

Південна Корея

У Південній Кореї питаннями безпеки у мережі переймається уряд, його рішення не переглядаються судами. Це робить процес непрозорим та вразливим для свавільного прийняття рішень. Південна Корея надає можливість посередникам та користувачам подавати апеляцію на рішення урядових органів, але вона рідко призводить до належного перегляду.

У лютому 2019 року Комісія комунікаційних стандартів Кореї підтвердила використання при блокуванні контенту (а саме порнографічних та піратських матеріалів) SNI-фільтрування, що передбачає моніторинг відвідуваних користувачами сайтів із HTTPS протоколами та блокування доступу до заборонених сайтів.

Постачальникам послуг, які не виконують накази Комісії, загрожує до двох років позбавлення волі або штраф до 20 мільйонів вон (приблизно 18083 долари США), відповідно до статті 73 Закону про сприяння використанню інформаційно-комунікаційних мереж та захисту інформації (Закон про мережу). Окремі особи, поліція та інші державні установи можуть доручити хостинг-провайдерам видалити контент. Отримуючи запит на видалення від окремих користувачів, компанія повинна негайно приховати відповідний контент на 30 днів і видалити його, якщо власник контенту не перегляне його або не оскаржить протягом цього часу, на підставі статті 44 (2).

Стаття 17 Закону про захист дітей та молоді покладає відповідальність за видалення зображень СЕНД на постачальників послуг із можливим покаранням у вигляді позбавлення волі на строк до трьох років або штрафом у розмірі до 20 мільйонів вон (приблизно 18083 долари США). У червні 2018 року Конституційний Суд підтримав статтю 17, зазначивши, що постачальники послуг за законом зобов'язані запобігати розповсюдженню зображень СЕНД.

Російська Федерація

У Російській Федерації веб-сайти можуть бути заблоковані відповідно до Закону про інформацію, інформаційні технології та захист інформації та відповідного галузевого законодавства. Заборонений контент включає зображення СЕНД; та низку іншого шкідливого контенту. Серед низки органів, які мають право обмежувати доступ до онлайн-контенту, виділимо Федеральне агентство з справ молоді, яке з вересня 2019 року отримало повноваження блокувати контент, який підбурює молодь до вчинення протиправної діяльності.

Інтернет-провайдери зобов'язані регулярно переглядати список заборонених сайтів, який оновлюється Роскомнаглядом. Засоби, за допомогою

яких Інтернет-провайдери повинні обмежувати доступ до веб-сайтів, не визначені, тому вони обмежують доступ за IP-адресами, доменними іменами, URL-адресами, чи фільтрують HTTPS-трафік, в тому числі використовуючи DPI-обладнання. Часто органи влади чітко не вказують конкретні сторінки, які вони хочуть заблокувати на певному веб-сайті. Відсутність чітких урядових вказівок іноді змушує провайдерів обмежувати доступ до найширшого кола веб-сайтів, щоб уникнути штрафів та загроз їх ліцензіям на діяльність. Пошукові системи та VPN також мають підключитися до списку Роскомнагляду та відповідно фільтрувати протиправні сайти.

У грудні 2020 року було підписано закон, що передбачає штрафи за невидалення контенту, забороненого Роскомнаглядом. Штрафи за перший випадок порушення становлять від 800 000 до 8 мільйонів рублів. Зрештою, штрафи за такі порушення можуть досягати п'ятої частини доходу компанії в Росії за календарний рік, що передує року, в якому було виявлено порушення.

Роскомнагляд не тільки додає певні URL-адреси до реєстрів заблокованих сайтів, а також їх доменні імена та IP-адреси, залишаючи оператору вирішувати, який із методів блокування використовувати. Блокування за URL-адресою є найменш інвазійним методом, і, як правило, оператори віддають перевагу саме йому. Однак цей метод вимагає використання додаткового обладнання, яке коштує дорого і часто недоступно для багатьох малих та середніх операторів. Крім того, якщо контент передається за допомогою зашифрованого протоколу HTTPS, провайдери та оператори зв'язку не можуть блокувати окремі веб-сторінки в домені, і їм нічого не залишається, як заблокувати або весь домен, або IP-адресу. Обидві дії призводять до одного і того ж наслідку: блокування суміжних правомірних ресурсів.

Висновки та рекомендації

Захист дітей від сексуальної експлуатації є легітимним та необхідним у будь-якому суспільстві. Поширення контенту, який містить СЕНД, завдає шкоди як дітям загалом, так і жертвам СЕНД у минулому.

Практика держав по всьому світу демонструє важливість міжнародної співпраці та активної протидії поширенню матеріалів СЕНД - через видалення контенту, який містить СЕНД, знаходження, підтримку та захист постраждалих від подібних посягань. Цим процесам можуть сприяти бази даних відомих зображень СЕНД (в тому числі для попередження повторного завантаження протиправного контенту) та взаємодія правоохоронних органів через гарячі лінії (INHOPE, IWF).

Видалення інших шкідливих для дітей матеріалів також починає ставати поширеним, в основному завдяки появі спеціальних органів з питань онлайн-безпеки. Вони видають обов'язкові до виконання приписи, підтримані суттєвими санкціями. Найбільш поширеним у цій категорії видом інформації, яку таргетують

відповідальні органи, є кібербулінг, трохи рідше контент, який може сприяти завданню собі шкоди.

Обмеження доступу до шкідливого контенту є найбільш логічним, коли хостинг-провайдер, який зберігає протиправний контент, перебуває у третій країні, яка не є членом найбільш активних гарячих ліній, ані активно співпрацює з українськими правоохоронними органами. Втім, його варто застосовувати лише у випадках, коли видалення такого контенту неможливе у першоджерелі розповсюдження.

На Україну ще очікує прийняття законодавства для протидії СЕНД. При його впровадженні, на нашу думку, для повноцінної відповідності стандартам, визначеними ЄСПЛ, та профільним Директивам ЄС варто використовувати наступні підходи:

1. Запровадити процедури, що дають змогу оперативно вилучати/видаляти матеріали, що зображують СЕНД, у разі, коли компанія підтверджує їхню наявність на її ресурсах. Можливість подавати скарги на відповідний матеріал мають отримати змогу як громадськість загалом, так і правоохоронні органи й організації, на базі яких функціонують гарячі лінії.
2. Якщо матеріали, що зображують СЕНД розміщено в іншій країні, однак не видалено з їхнього джерела, Інтернет-провайдери мають використовувати доступні їм технічні засоби для блокування чи фільтрування таких матеріалів, аби перешкодити доступу до нього. При цьому, вони мають:
    a. використовувати методи блокування найбільш сумісні з стандартами прав людини (за DNS чи URL-адресами, за IP-адресами лише коли буде заблоковано виключно протиправний ресурс; уникати методів, які диспропорційно впливають на право на приватність);
    b. забезпечити доступність адміністративної та судової процедури оскарження блокування;
    c. повідомляти користувачів про причини блокування, якщо це не становить загрози для постраждалих осіб чи розслідування;
    d. забезпечити можливість оперативної зміни адрес блокування через спроби уникнення постачальниками протиправного контенту та періодичне оновлення бази заблокованих ресурсів.
3. Використовувати механізми повідомлення та реагування, включаючи використання найбільших міжнародних гарячих ліній та їх інструментів.
4. Наділити окремий державний орган повноваженнями отримувати та розглядати скарги у зв’язку з випадками СЕНД та звертатися до організацій, які розміщують контент, для видалення відповідних матеріалів, або створити новий державний орган з відповідними повноваженнями.

5. Розробити спрощений механізм видалення матеріалів, що зображують СЕНД, хостинг-провайдерами та Інтернет-провайдерами, а також забезпечити можливість блокування ресурсів, що систематично поширюють такий контент, у позасудовому порядку (за зверненням Кіберполіції або органу, який виконуватиме функції забезпечення онлайн безпеки). При цьому, необхідно відобразити усі елементи цих процедур безпосередньо у тексті закону, що такі процедури впроваджуватиме.
6. Впровадити механізми прозорості, зокрема публікувати інформацію щодо кількості ресурсів, до яких обмежено доступ, кількості запитів до іноземних правоохоронних органів (напряму чи через гарячі лінії), кількості вилученого контенту, оцінки кількості постраждалих від СЕНД дітей та процесу надання їм психологічної та іншої допомоги тощо.

Аналітичний звіт підготовлений за підтримки Американської Асоціації Юристів Ініціативи з Верховенства Права (ABA ROLI) в Україні.