Проєкт Ради Європи «Підтримка впровадження європейських стандартів прав людини в Україні»

АНАЛІЗ НАЦІОНАЛЬНИХ ПРАВОВИХ МЕХАНІЗМІВ ПОПЕРЕДЖЕННЯ НЕЗАКОННОГО РОЗПОВСЮДЖЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

Підготовлений:
Маркіяном Бемом, експертом Ради Європи
Іваном Городиським, експертом Ради Європи

Київ - 2023

Зміст

А. Загальний опис проблеми

Станом на сьогодні Офісом Уповноваженого Верховної Ради України з прав людини на підставі звернень громадян, а також за результатами реалізації інших повноважень з контролю за додержанням законодавства про захист персональних даних, ідентифіковано низку проблем, пов'язаних із масовим незаконним поширенням (збором) персональних даних у мережі інтернет.

До цих проблем, серед іншого, належать такі:

- поширення персональних даних громадян України, зокрема військовослужбовців[1];
- поширення персональних даних українських військовослужбовців, поєднане з поширенням дезінформації, неправдивої інформації та інформації, що носить характер обвинувачення у вчиненні злочину[2];
- використання з різними цілями фішингових інтернет ресурсів[3];
- поширення персональних даних, що очевидно порочать честь, гідність та ділову репутацію фізичних осіб.

Перелічені проблеми несуть серйозну загрозу правам окремих осіб та інтересам держави. У такій категорії справ важливу роль відіграє швидкість реагування та усунення порушення. Чим тривалішим буде час перебування поширеної інформації у вільному доступі, тим серйозніші наслідки це матиме для прав потерпілих та/чи держави.

Часто такі дії містять ознаки кримінального чи адміністративного правопорушення. Однак, навіть ефективне розслідування такого правопорушення може забрати надміру тривалий час. Більш того, часто причетних осіб складно, а то і зовсім неможливо, встановити. Наприклад, поширення відомостей на веб-сайтах зареєстрованих за межами країни суттєво ускладнює, якщо не унеможливлює, встановлення відповідальних осіб.

Згідно з усталеною практикою Європейського суду з прав людини (далі - ЄСПЛ) поширення чи фіксація чутливих відомостей про фізичну особу є серйозним втручанням в право такої особи на повагу до її приватного життя. Відсутність належного реагування (зокрема проведення ефективної перевірки чи розслідування) на такі дії з боку держави може становити порушення ст. 8 Конвенції про захист прав і основоположних свобод людини (далі – Конвенція). В якості найбільш яскравих прикладів можна навести рішення ЄСПЛ у справах *I v. Finland* (заява № 20511/03), *K.U. v. Finland* (заява № 2872/02) та *Söderman v. Sweden* (заява № 5786/08).

Відтак, чинне законодавство повинно містити механізми, покликані з одного боку недопустити погіршення ситуації до завершення розслідування (перевірки, розгляду справи та ін.), а з іншого припинити дії, що містять ознаки очевидного порушення.

---

[1] Див. www.nemez1da.ru;

[2] Див. https://ukrsof.wordpress.com/, https://tribunal.ru/, https://www.pacifistru.com/nazi/, https://украинские-преступления.org/#p=112 та https://myrotvorets.center ;

Найбільш очевидним та ефективним механізмом реагування на ситуації масового незаконного поширення (чи збору) персональних даних в мережі інтернет було б тимчасове чи постійне блокування відповідного веб-ресурсу (URL-адреси, веб-сайту, IP-адрес та ін.). У зв'язку із цим доцільно проаналізувати наявні на національному рівні механізми реагування на перелічені вище ситуації.

В. Існуючі засоби захисту

Офіс Уповноваженого Верховної Ради України з прав людини неодноразово звертався до інших органів державної влади з клопотанням про блокування тих чи інших веб-ресурсів. Йдеться зокрема про Адміністрацію Державної служби спецзв'язку та захисту інформації.

Аналіз чинного законодавства та адміністративної практики засвідчує наявність у національних органів влади реальних механізмів блокування інтернет ресурсів. На практиці блокування передбачає унеможливлення перетворення імені сайту на його IP-адресу. Блокуватись може доступ як до IP-адрес, так і автономної системи. Даною можливістю володіють провайдери послуг електронної комунікації.

Станом на сьогодні в Україні застосовуються чотири основні юридичні механізми блокування веб-ресурсів:

- Санкції;
- Розпорядження Національного центру оперативно-технічного управління електронними комунікаційними мережами України;
- Система фільтрації фішингових доменів;
- Рішення Національної ради України з питань телебачення і радіомовлення.

Законодавчі підстави функціонування вказаних механізмів виглядають досить непевними.

1. Використання санкцій, як механізму блокування вебресурсів було вперше використано у 2017 році. Указом Президента України №133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» було застосовано такий вид обмежувального заходу як «заборона Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів». Вказаний вид санкції було застосовано до низки веб-ресурсів, таких як «Одноклассники», «Доктор Веб», «ВКонтакте», «Антивирус Касперского», «Яндекс» та «Mail.ru»[4]. В подальшому такі обмежувальні заходи було застосовано ще у декількох указах Президента України.

На той момент чинним законодавством не було передбачено такого виду санкції. Однак, як відомо коло санкцій, передбачених Законом не є вичерпним. Пунктом 25 ч. 1 ст. 4

[4] Див. https://www.president.gov.ua/storage/j-files-storage/00/40/38/6f76b8df9d0716da74bb4ae6a900d483_1494964345.pdf

Закону України «Про санкції» передбачено «*інші санкції, що відповідають принципам їх застосування, встановленим цим Законом*».

В подальшому до Закону України «Про санкції» були внесені зміни, якими запроваджено нові види санкцій, що вже передбачали можливість блокування веб-ресурсів. Станом на сьогодні пп. 9 та 24-5 ч. 1 ст. 4 вказаного Закону передбачено можливість застосування санкцій у вигляді «*обмеження або припинення надання електронних комунікаційних послуг і використання електронних комунікаційних мереж*» та «*заборони демонстрації та використання символіки терористичних організацій і груп, пропагування ідей та програмних цілей таких організацій (груп), блокування доступу до інформаційних ресурсів, які використовуються для зазначених цілей*».

Разом з тим, якихось чітких механізмів виконання рішень, якими застосовано вказані санкції, відповідним Законом не передбачено.

2. Розпорядження Національного центру оперативно-технічного управління електронними комунікаційними мережами України. Статтею 29 Закону України «Про телекомунікації» (втратив чинність з прийняттям Закону України «Про електронні комунікації» в грудні 2020 року) було передбачено створення та діяльність Національного центру оперативно-технічного управління мережами телекомунікацій (далі – Національний центр). Порядок створення та діяльності Національного центру повинен був визначатись Кабінетом Міністрів України (далі - КМУ). На виконання вказаного положення КМУ було прийнято Постанову від 29 червня 2004 р. N 812 «Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану», якою було затверджено Порядок оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану (далі – Порядок управління).

Видається, що вказаний центр було створено лише розпорядженням КМУ від 27 березня 2019 р. № 177-р Київ «Про утворення Національного центру оперативно-технічного управління мережами телекомунікацій». Згідно з п. 1 вказаного розпорядження Національний центр створено як державну установу «у межах загальної чисельності особового складу» Адміністрації Державної служби спеціального зв'язку та захисту інформації[5].

В грудні 2020 року було прийнято Закон України «Про електронні комунікації», який прийшов на заміну Закону України «Про телекомунікації». Частина перша та третя ст. 32 Закону України «Про електронні комунікації» містить положення аналогічні тим, що містились у ст. 29 Закону України «Про телекомунікації».

В травні 2022 року ст. 32 Закон України «Про електронні комунікації» доповнено частиною восьмою. Згідно з вказаним положенням Національний центр в умовах надзвичайного або воєнного стану видає розпорядження щодо оперативно-технічного

[5] Див. https://www.kmu.gov.ua/npas/pro-utvorennya-nacionalnogo-centru-operativno-tehnichnogo-upravlinnya-merezhami-telekomunikacij?fbclid=IwAR193oYU-H-p9uYbpySwD6FS6UBR6a8YjRFbOZNKq4uw8orSD6gVmljAt58

управління електронними комунікаційними мережами, які є обов’язковими для виконання постачальниками електронних комунікаційних мереж та/або послуг. Також, під час дії воєнного стану на підставі звернення Національного центру регуляторний орган може прийняти за погодженням з КМУ рішення про виключення з реєстру постачальників електронних комунікаційних мереж та послуг тих постачальників, які не виконали розпорядження Національного центру оперативно-технічного управління електронними комунікаційними мережами України.

Більш детально повноваження Національного центру викладено у Порядку управління. Згідно з п. 27 Порядку управління Національний центр в умовах надзвичайних ситуацій, надзвичайного та воєнного стану видає розпорядження щодо оперативно-технічного управління телекомунікаційними мережами, які є обов'язковими для виконання центрами управління мережами. Вказані розпорядження є обов’язковими до виконання. Також згідно з п. 14 Національний центр та центри управління мережами за погодженням з Адміністрацією Держспецзв'язку відповідно до законодавства можуть допускати деяке зниження якості послуг та встановлювати тимчасові обмеження щодо їх надання до ліквідації надзвичайних ситуацій, скасування надзвичайного та воєнного стану.

Чинним законодавством прямо не передбачено права Національного центру приймати рішення щодо блокування інтернет ресурсів. Навпаки, основним завданням центру є підтримання сталого функціонування та координування роботи електронних мереж в умовах, серед іншого, воєнного стану. Однак, керуючись вказаними нормами чинного законодавства, після запровадження воєнного стану Національний центр розпочав видавати розпорядження щодо блокування веб-сайтів[6]. Вже в перші дні повномасштабного вторгнення Національним центром видано розпорядження щодо блокування 709 доменів та їх піддоменів (автономних систем). У такий спосіб було заблоковано доступ до понад 40 мільйонів IP-адрес з російського сегменту мережі[7].

Такі розпорядження Національного центру доводяться до відома Інтернет провайдерів регулятором сфери електронних комунікацій – Національною комісією, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв’язку[8].

Очевидно, що з огляду на те, що невиконання відповідного розпорядження Національного центру може мати наслідком втрату ліцензії на здійснення діяльності з надання комунікаційних послуг, усі інтернет провайдери їх виконуватимуть.

3. Система фільтрації фішингових доменів. Розпорядженням Національного центру від 30.01.2023 року № 67/850 було створено систему фільтрації фішингових доменів (далі - Система), як складової Національного сервісу доменних імен (DNS). Вказаним документом також затверджено Регламент роботи системи фільтрації фішингових доменів.

[6] Див. https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2604&language=uk
[7] Див. https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2282&language=uk
[8] Див. попередні посилання.

Згідно з Регламентом метою Системи є фільтрація фішингових доменів з метою протидії шахрайству в банківській та фінансовій сфері. Фішингові домени імітують офіційні веб-ресурси фінансових установ, інтернет-магазинів та інше. Інформація, яку користувачі вводять на вказаних веб-ресурсах використовується зловмисниками з метою заволодіння коштами вказаних осіб.

Для запобігання таким ситуаціям і створено Систему, яка покликана автоматично блокувати такі фішингові домени. Для цього національні провайдери DNS реєструються в Системі та отримують у такий спосіб доступ до переліку фішингових доменів. Вказана система оновлюється кожних 15 хвилин, підвантажуючи перелік шкідливих інтернет-ресурсів. В подальшому Система автоматично блокує будь-які спроби відвідати вказані веб-сайти через DNS сервери провайдерів.

Відповідальність за ведення обліку фішингових доменів несе галузева команда реагування на кіберінциденти у банківській системі України Національного Банку України (CSIRT-NBU). Для зберігання та розповсюдження переліку цих доменів використовується спеціально виготовлена для цього платформа MISP. Працівники CSIRT-NBU розглядають звернення щодо поповнення вказаного переліку доменів від учасників Системи (національних провайдерів DNS) та суб'єктів забезпечення кібербезпеки України (сюди зокрема належать Служба безпеки України та Адміністрація Держспецзв'язку).

4. Рішення Національної ради України з питань телебачення і радіомовлення. 13 грудня 2022 року було прийнято Закон України «Про медіа». Вказаним інструментом запроваджено новий механізм блокування веб-ресурсів. З огляду на відносну новизну закону, практики застосування цього механізму на разі не виявлено, однак положення чинного законодавства дають розуміння щодо його суті.

Також, згідно з п. 15 ч. 3 ст. 18 Закону України «Про електронні комунікації» Національна рада України з питань телебачення і радіомовлення (далі – Національна рада) та суд мають право обмежувати доступ до веб-сайтів шляхом застосування постійної чи тимчасової заборони поширення онлайн-медіа.

Крім цього, згідно з ч. 2 ст. 123 Закону України «Про медіа» Національна рада затверджує та оновлює *Перелік аудіовізуальних медіа-сервісів на замовлення та сервісів провайдерів аудіовізуальних сервісів держави-агресора*. Такий Перелік є відкритим та підлягає оприлюдненню на веб-сайті Національної ради. Відповідно до п. 16 ч. 3 ст. 18 Закону України «Про електронні комунікації» та ч. 8 ст. 123 Закону України «Про медіа» рішення Національної ради про внесення сервісу до Переліку, якщо такий сервіс надається за допомогою веб-сайту, тягне за собою обмеження доступу до відповідного веб-сайту.

Згідно з ч. 1 ст. 99 Закону України «Про медіа» заборона поширення онлайн-медіа за рішенням Національної ради або за рішенням суду в порядку є одним з передбачених законом заходів реагування на порушення вимог законодавства та/або умов ліцензії.

Підстави та порядок застосування вказаного заходу реагування детально викладено у ст. 112 та 116 Закону України «Про медіа». Зазвичай застосування вказаного заходу є

відповіддю на неодноразові значні та грубі порушення положень вказаного закону. Детальний перелік значних та грубих порушень викладено в ст. 112 Закону.

Також ст. 115-1, 115-2 та 116 Закону «Про медіа» визначають процедуру застосування вказаного заходу реагування. Так, у разі застосування вказаного заходу реагування Національна рада впродовж трьох робочих днів з дати прийняття відповідного рішення Національною радою чи з дати отримання відповідного судового рішення, яке набрало законної сили, повідомляє Регулятора комунікаційних послуг про веб-сайт, доступ до якого підлягає обмеженню постачальниками електронних комунікаційних послуг.

Регулятор комунікаційних послуг впродовж трьох робочих днів з дати отримання повідомлення Національної ради інформує постачальників електронних комунікаційних послуг через електронну регуляторну платформу про обов'язок обмеження доступу до веб-сайтів, визначених у повідомленні Національної ради.

Постачальники електронних комунікаційних послуг зобов'язані впродовж трьох робочих днів з дня отримання повідомлення Регулятора комунікаційних послуг обмежити доступ до відповідного веб-сайту на території України.

Висновок: чинним законодавством передбачено низку правових механізмів блокування інтернет ресурсів. Таке блокування здійснюється у випадках 1) порушення законодавства про медіа, 2) вчинення дій, що тягнуть за собою накладення санкцій, 3) вчинення фінансових чи банківських махінацій та 4) забезпечення сталого функціонування електронних мереж.

На практиці функціонування вказаних механізмів, за винятком блокування, передбаченого законодавством про медіа, характеризується відсутністю будь-яких процесуальних гарантій дотримання прав власників заблокованих веб-ресурсів. Фактично ці механізми побудовані таким чином, що будь-який веб-ресурс може бути заблоковано без наведення підстав такого рішення і відповідного обґрунтування, та без чітких механізмів оскарження. Найбільш яскравим прикладом у цьому відношенні є діяльність Національного центру, який формально не володіє повноваженнями по блокуванню веб-сайтів, однак блокує веб-сайти будь-якого характеру та володіє фактично необмеженими повноваженнями у цій сфері.

Обмеження доступу до веб-ресурсів Національною радою України з питань телебачення і радіомовлення є більш передбачуваним. В першу чергу сама Національна рада може розглядатись в якості незалежного органу, оскільки її склад формується Президентом України та Верховною Радою України. Крім цього, законодавство містить чіткий перелік підстав для застосування такого засобу реагування, а рішення Національної ради можуть бути оскаржені до суду.

У цьому зв'язку доцільно також проаналізувати міжнародний досвід з питань блокування веб сайтів.

С. Міжнародні інструменти та практика Європейського суду з прав людини.

Практика ЄСПЛ з питань щодо стосуються блокування Інтернет ресурсів почала сформуватись відносно недавно. Попри те, що рішень ЄСПЛ з цього приводу не так вже й багато, підхід Суду до розгляду таких справ є чітким та однозначним і ґрунтується на принципах, сформованих у справах за ст. 10 Конвенції. З огляду на вказані обставини, нижче наводиться аналіз ключових рішень ЄСПЛ з питань, що є предметом даного дослідження. За результатами аналізу вказаних рішень наведено загальні висновки щодо вимог, які ставляться Судом, до функціонування системи блокування Інтернет ресурсів.

Ахмет Їлдірім проти Туреччини (Ahmet Yıldırım v. Turkey) (рішення від 18 грудня 2012 року)[9]

Факти:

Заявник володіє та керує веб-сайтом (http://sites.google.com/a/ahmetyildirim.com.tr/academic/), на якому він публікує свої наукові роботи. Сайт розташований на Google Sites. 23 червня 2009 р. згідно з законом про регулювання публікацій в Інтернеті та боротьбу з правопорушеннями в Інтернеті, кримінальний суд першої інстанції постановив заблокувати веб-сайт№ http://sites.google.com/site/kemalizminkarinagrisi/benimhikayem/atatuerk-koessi/at як запобіжний захід щодо власника сайту, якого звинуватили в образі пам'яті Ататюрка.

На наступний день суд змінив рішення та наказав заблокувати весь доступ до Google Sites. Управління телекомунікацій та інформаційних технологій («TİB») зазначив, що це був єдиний спосіб заблокувати конкретний веб-сайт, оскільки його власник не мав сертифіката сервера та проживав за кордоном. У результаті був заблокований весь доступ до Google Sites.

Заявник оскаржував блокування, зокрема зазначаючи, що його сайт не був пов'язаний із сайтом-порушником, однак марно. Згодом кримінальне провадження було припинено, однак захід блокування залишився в силі.

Мотивація Суду:

Оскаржуваний захід становив обмеження, що випливає з запобіжного заходу - блокування доступу до Інтернет-сайту. З метою його виконання суд наказав заблокувати доступ до Google Sites, на яких також розміщено веб-сайт заявника. Таким чином, заявник був позбавлений доступу до власного веб-сайту. Цієї обставини достатньо для того, щоб визнати захід блокування «втручанням органів державної влади» у право заявника на свободу вираження поглядів, невід'ємною частиною якого є свобода отримувати та передавати інформацію та ідеї.

Блокування доступу до веб-сайту мало законодавчу основу. Однак для задоволення вимог Конвенції **закон має достатньо чітко вказувати обсяг будь-якого такого дискреційного права (зокрема виконавчої влади) та спосіб його використання**. У цьому

[9] Див. https://hudoc.echr.coe.int/eng?i=001-115705

випадку закон передбачав, що суддя може видати розпорядження про блокування доступу до «**інтернет-публікації**, якщо є достатні підстави підозрювати, що їхній зміст є таким, що становить ... правопорушення». Незважаючи на те, що поняття «публікація» виглядає дуже широким, очевидно, що ні веб-сайт заявника, ні Google Sites як такі не підпадають під значення цього поняття.

Факти справи свідчать про те, що **ТІВ міг вимагати розширення обсягу наказу** про блокування, навіть якщо проти відповідного веб-сайту чи домену не було порушено жодних судових процесів і не було встановлено реальної потреби в повному блокуванні. При цьому, **національні суди просто послалися на рекомендацію ТІВ щодо блокування всієї платформи Google Sites, не встановивши:**

- чи можна було вжити менш далекосяжні заходи, щоб заблокувати доступ конкретно до веб-сайту-порушника;

- наявність необхідності блокування повного доступу до Google Sites, зважаючи на інтереси усіх зацікавлених сторін;

- чи матиме захід блокування свавільні наслідки.

Зважаючи на це, ЄСПЛ знайшов порушення статті 10.

Ченгіз та інші проти Туреччини (Cengiz and Others v. Turkey) (рішення від 18 грудня 2012 року)[10]

Факти:

Кримінальний суд першої інстанції Анкари на підставі закону видав наказ про блокування доступу до www.youtube.com та IP-адрес 208.65.153.238 до 208.65.153.251, що забезпечує доступ до сайту. Суд постановив, серед іншого, що вміст десяти сторінок на веб-сайті (десять відеофайлів) порушує Закон про заборону наруги над пам'яттю Ататюрка.

Заявники подали заперечення проти наказу про блокування, стверджуючи, що блокування такого доступу серйозно порушило саму суть їхнього права на свободу отримувати інформацію та ідеї. Крім того, 6 із 10 сторінок, яких стосувався наказ уже були видалені, а інші чотири більше не були доступні з території Туреччини.

Кримінальний суд першої інстанції Анкари відхилив заперечення заявників. Апеляція залишила наказ в силі.

У подальшому було ухвалено ще одне рішення щодо блокування веб-сайту www.youtube.com та 44 інших IP-адрес, що належать сайту. Увесь процес оскарження повторився.

Мотивація Суду:

Чи можуть заявники вважатися «жертвами»?

Заявники подали свої заяви до нього як активні користувачі YouTube; серед іншого, вони звернули увагу на наслідки наказу про блокування для їхньої академічної роботи та на

[10] Див. https://hudoc.echr.coe.int/eng?i=001-159188

важливі особливості відповідного веб-сайту. Вони, зокрема, заявили, що через свої облікові записи на YouTube вони використовували платформу не лише для доступу до відео, що стосуються їх професійної сфери, але й активно для завантаження та обміну файлами такого характеру.

YouTube не лише розміщує художні та музичні твори, але також є дуже популярною платформою для політичних промов та політичної та соціальної діяльності. Відповідно, **вжитий захід заблокував доступ до веб-сайту, який містив конкретну інформацію, що представляла інтерес для заявників, і до якої було важко отримати доступ іншими засобами**.

Крім того, після подання заяв, Конституційний суд Туреччини у справі щодо адміністративного рішення про блокування доступу до YouTube надав статус потерпілих деяким активним користувачам сайту, серед яких другий і третій заявники.

Оскільки, зважаючи на функції YouTube, наказ про блокування позбавив заявників значних засобів здійснення свого права на свободу отримувати та передавати інформацію та ідеї, Суд визнає їх «жертвами».

Чи було втручання?

Стаття 10 стосується не лише змісту інформації, а й засобів розповсюдження, оскільки будь-яке обмеження, накладене на такі засоби, обов'язково втручається в право отримувати та поширювати інформацію. Подібним чином Суд підтверджує, що стаття 10 гарантує не лише право на поширення інформації, але й **право громадськості отримувати її**.

У цій справі через блокування заявники не мали доступу до YouTube протягом тривалого періоду. Тому як активні користувачі YouTube вони можуть законно стверджувати, що відповідний захід вплинув на їхнє право отримувати та передавати інформацію та ідеї.

Чи було втручання виправданим?

Блокування доступу до веб-сайту мало підставу в законі лише в частині конкретного забороненого контенту. Оскільки технологія фільтрації URL-адрес для іноземних веб-сайтів недоступна в Туреччині, для виконання рішення щодо конкретного контенту, **адміністративний орган вирішив заблокувати будь-який доступ до всього веб-сайту**. Однак **влада повинна була взяти до уваги, що такий захід зробить велику кількість інформації недоступною, а тому суттєво обмежить права користувачів Інтернету**.

Отже, **захід блокування не задовольняв вимогу передбачуваності закону** та не надавав заявникам того ступеня захисту, на який вони мали право відповідно до верховенства права в демократичному суспільстві.

У зв'язку з цим **мало місце порушення статті 10 Конвенції**.

****Важливо: Суд порівнював обставини цього кейсу з двома попередніми, у яких порушення не було визнано - Tanrıkulu and Others v. Turkey (№ 40150/98, від 6 листопада***

2001)[11] та Akdeniz v. Turkey (№ 20877/10, від 11 березня 2014)[12]. Різниця в тому, що заявники (читачі забороненої газети та користувачі сайту з піратською музикою) не були жертвами у розумінні Конвенції, бо лише опосередковано постраждали від заборон. Інформацію про новини та музику, яку аудиторія одержувала з цих двох джерел, можна було легко одержувати з інших – легальних – джерел. Застосовані заходи обмеження у цих випадках ніяк не обмежили професійної чи унікальної діяльності заявників.

Вікімедія Фаундейшн проти Туреччини (Wikimedia Foundation, Inc. v. Turkey) (рішення від 1 березня 2022 року)[13]

Факти:

Заявник, фонд Wikimedia Foundation, Inc., присвячений вільному обміну знаннями безкоштовну онлайн-енциклопедію. У 2017 році Генеральний директорат безпеки при офісі прем'єр-міністра звернувся до Директорату телекомунікацій та інформаційних технологій (ТІВ) з проханням видалити дві сторінки з веб-сайту Вікіпедії: *«Спонсорований державою тероризм»* і *«Іноземна участь у громадянській війні в Сирії»*.

Того ж дня Фонд Вікімедіа отримав вимогу від ТІВ видалити п'ять URL-адрес протягом чотирьох годин. Зазначені сторінки не були видалені протягом цього терміну. Оскільки технічно неможливо заблокувати доступ лише до цих сторінок, ТІВ наказав заблокувати доступ до всього веб-сайту.

Суд залишив рішення в силі, подальші апеляції були відхилені.

Конституційний суд постановив, що мало місце порушення статті 26 Конституції, яка захищає право на свободу вираження поглядів: захід не ґрунтувався на нагальній суспільній потребі, наведені причини були недостатніми та становили непропорційне втручання у право на свободу вираження поглядів. Перший магістратський суд Анкари негайно скасував наказ про блокування доступу до всього сайту Вікіпедії. Заявник подав заяву до ЄСПЛ, поки його індивідуальне звернення до Конституційного Суду перебувало на розгляді.

Мотивація Суду:

У цій справі захід, на який скаржився фонд-заявник, а саме наказ про блокування доступу до веб-сайту Вікіпедії, спочатку виданий ТІВ, адміністративним органом, а згодом підтриманий компетентним магістратським судом, був скасований 15 січня 2020 року після повідомлення рішення Конституційного суду від 26 грудня 2019 року. Перший магістратський суд вирішив негайно скасувати наказ про блокування доступу до всього веб-сайту Вікіпедії. Стосовно ефективності індивідуальної заяви до Конституційного Суду, Суд зауважив, що в численних справах щодо свободи вираження поглядів він визнав, що заява

[11] https://hudoc.echr.coe.int/?i=001-43109
[12] https://hudoc.echr.coe.int/?i=001-142383
[13] https://hudoc.echr.coe.int/?i=001-216677

такого роду повинна розглядатися як засіб правового захисту, який необхідно вичерпати для цілей статті 35 § 1 Конвенції щодо таких скарг. Суд не бачив підстав відступати від цієї прецедентної практики, оскільки не було достатньо доказів для висновку про те, що індивідуальна заява до Конституційного Суду не могла забезпечити належне відшкодування скарги фонду-заявника за статтею 10 Конвенції. Насамперед щодо правил блокування доступу до веб-сайтів відповідно до розділу 8/A Закону №. 5651, з рішень Конституційного суду було зрозуміло, що цей суд встановив лінію прецедентного права, яка визначає критерії, які слід застосовувати. Зокрема, Конституційний суд постановив, що блокування доступу до всього веб-сайту є винятковим заходом, і він перерахував критерії, які повинні застосовуватися при прийнятті рішення про такі заходи. Після розгляду справи він також встановив, що захід, призначений адміністративними та судовими органами, не ґрунтувався на нагальній суспільній потребі, що для цього не було надано достатніх причин і що він становив непропорційне втручання у право на свободу вираження поглядів. Суд взяв до уваги аргументи фонду-заявника та зауваження третіх сторін щодо системного характеру проблеми, порушеної у цій справі. Тим не менш, у нього не було достатньо відповідної інформації, щоб припустити, що Конституційний суд не спроможний вирішити стверджувану системну проблему. Як визнав фонд-заявник, Конституційний суд виніс кілька рішень щодо блокування веб-сайтів, за допомогою яких він встановив велику кількість критеріїв, яких повинні дотримуватися національні органи влади та суди, покликані розглядати накази про блокування. Крім того, якщо було доведено, що проблема має системний характер, **Конституційний Суд також мав у своєму розпорядженні відповідні засоби, такі як процедура пілотного рішення, як альтернативу простому встановленню порушення в даній справі**. Подібним чином, розглядаючи індивідуальну заяву, Конституційний Суд мав **повноваження оцінювати передбачуваність положення, яке розглядається, і, якщо доречно, виявляти, що воно не відповідає вимогам щодо «якості закону»**.

Стосовно тривалості провадження в Конституційному суді Суд зазначив, що Конституційний суд виніс своє рішення через два роки і вісім місяців після подання індивідуальної заяви. На думку Суду, хоча це був тривалий період, він не був явно надмірним, особливо з огляду на те, що було поставлено на карту у справі.

З огляду на це заяву Суд визнав неприйнятною.

Таганрог ЛРО та інші проти Росії (Taganrog LRO and Others v. Russia) рішення від 7 червня 2022 року

Факти:

У серпні 2013 року Центральний районний суд визнав сайт Свідків Єгови екстремістським через розміщення на ньому примірників брошур, визнаних екстремістськими, і примірників видань журналів, дозвіл на розповсюдження яких було скасовано. Наступного місяця нью-йоркське Товариство «Вартова башта» (власник міжнародного веб-сайту Свідків Єгови), адміністративний центр і десять окремих

російських Свідків Єгови з вадами зору чи слуху подали окремі апеляції, скаржачись на те, що вони не мали можливості взяти участь у розгляді; що рішення заблокувати доступ до всього веб-сайту перешкоджало вірянам у росії отримати доступ до інших матеріалів, і що веб-сайт був єдиним джерелом релігійних матеріалів із коментарями мовою жестів або аудіозаписами для сліпих користувачів. Апеляція була безуспішною. У липні 2015 року Міністерство юстиції внесло сайт до Федерального списку екстремістських матеріалів.

Мотивація Суду:

Суд знайшов **порушення статті 10 в поєднанні зі ст. 9 Конвенції**. Обмеження доступу до веб-сайту Свідків Єгови з території Росії було рівнозначне «втручанню державного органу» у право власника веб-сайту Watchtower New York поширювати інформацію серед окремих Свідків Єгови та інших зацікавлених осіб у Росії. Цей захід також перешкоджав адміністративному центру отримувати та передавати інформацію своїм членам. Для заявників із вадами зору чи слуху веб-сайт був **єдиним доступним джерелом релігійних матеріалів**, які можна було завантажити, що стосувалися їхніх конкретних потреб. Крім того, Watchtower New York не отримала **попереднього попередження або можливості видалити з веб-сайту нібито незаконний матеріал**. Організацію також не запросили взяти участь у наступному слуханні. Суд визнав, що рішення заблокувати доступ до всього веб-сайту було незаконним і непропорційним, тим більше, що Watchtower New York в результаті видалила образливі публікації.

Володимир Харітонов проти Росії (Vladimir Kharitonov v. Russia) (рішення від 23 червня 2020 року)[14]

Факти:

Наприкінці 2012 року заявник виявив, що IP-адреса його сайту Electronic Publishing News (www.digital-books.ru) була заблокована телекомунікаційним регулятором Роскомнагляд. Цю міру було вжито після рішення Федеральної служби з контролю за наркотиками, яка хотіла заблокувати доступ до іншого веб-сайт: www.rastaman.tales.ru – збірки народних оповідань на тему канабісу, який мав ту саму хостингову компанію та IP-адресу, що й веб-сайт заявника. Копії рішень про блокування та розблокування не були надані ні заявнику, ні Суду.

Заявник подав скаргу до суду, стверджуючи, що блокування IP-адреси також заблокувало доступ до його веб-сайту, який не містив жодної незаконної інформації. Суди визнали, що Роскомнагляд діяв у межах своєї компетенції з метою захисту дітей від шкідливої інформації про вживання наркотиків, без оцінки їх впливу на сайт заявника.

Мотивація Суду:

[14] https://hudoc.echr.coe.int/eng?i=001-203177

Заявник був власником і адміністратором веб-сайту (який має спільну цифрову мережеву адресу («IP-адресу») з багатьма іншими веб-сайтами на тому ж сервері), на якому розміщено контент, пов'язаний із виробництвом і розповсюдженням електронних книг, від новин до аналітичних звітів і практичних посібників.

Наслідки заходу для Заявника полягали в тому, що він: не знав про підстави для блокування або його тривалість; не міг контролювати, коли ці заходи будуть скасовані, а доступ до його сайту буде відновлено; не міг поділитися останніми подіями та новинами про електронне видавництво, а відвідувачі його веб-сайту не мали доступу до всього вмісту веб-сайту.

Конвенція вимагає, щоб втручання у вигляді блокування сайту відповідало вимогам, у тому числі було «передбачено законом». **Закон мав бути, серед іншого, чітким і передбачуваним; встановити межі дискреційних повноважень влади; забезпечити захист від свавільного втручання**. Однак у цьому кейсі веб-сайт заявника було заблоковано відповідно до статті 15.1 Закону про інформацію, яка перелічувала категорії незаконного веб-контенту та надавала Роскомнагляду широкі повноваження щодо виконання наказу про блокування. При цьому, закон не вимагав від Роскомнагляду **перевіряти, чи використовується ця адреса кількома веб-сайтами, або встановлювати необхідність блокування за IP-адресою**.

Сам же веб-сайт заявника не містив жодних незаконних матеріалів, а був заблокований лише тому, що він мав ту саму IP-адресу, що й веб-сайт, який насправді містив незаконні матеріали. Російське законодавство **не вимагає від заявника контролю за вмістом спільно розміщених веб-сайтів або дотриманням постачальником послуг хостингу наказів про видалення**. Проте **через широкі повноваження Роскомнагляду щодо блокування, заявнику довелося нести наслідки рішення влади про блокування** лише через випадковий зв'язок на рівні інфраструктури між його веб-сайтом і чужим незаконним контентом.

Отже, втручання у право пана Харитонова не було обґрунтовано жодним законом. Більш того, російське законодавство не передбачало жодної оцінки впливу блокувального заходу до його впровадження, а також сповіщення третіх сторін про рішення щодо блокування за обставин, коли вони мають побічний вплив на права інших власників веб-сайтів. Крім того, це виявилося системною проблемою: **мільйони веб-сайтів блокувалися в росії лише з тієї причини, що вони ділили одну IP-адресу з іншими веб-сайтами з незаконним вмістом**.

Таким чином, було визнано порушення статті 10 Конвенції.

ООО Флавус та інші проти Росії (OOO Flavus and Others v. Russia) (рішення від 23 червня 2020 року)[15]

Факти:

[15] https://hudoc.echr.coe.int/eng?i=001-203178

Заявники володіли опозиційними ЗМІ: www.grani.ru, www.kasparov.ru та щоденною газетою «Ежедневный журнал» на сайті www.ej.ru, яка публікує дослідження та аналітику з критикою російського уряду. У березні 2014 року Роскомнадзор заблокував доступ до веб-сайтів заявників на вимогу Генеральної прокуратури, діючи відповідно до статті 15.3 Закону про інформацію, через контент, який нібито пропагував масові заворушення або екстремістські висловлювання. Жодної ухвали суду не було потрібно. Заявники безуспішно подали клопотання про судовий перегляд заходу блокування, скаржачись на повне блокування доступу до їхніх веб-сайтів і відсутність повідомлення про конкретні образливі матеріали, які вони не могли видалити, щоб відновити доступ.

Мотивація Суду:

<u>Чи було блокування законним:</u>

Веб-сайти ТОВ «Флавус та інші» були заблоковані згідно зі статтею 15.3 Закону про інформацію, яка **дозволяла Генеральній прокуратурі вимагати блокування різного типу контенту**, зокрема закликів до масових заворушень або участі в несанкціонованих публічних заходах. Оскільки повідомлення Роскомнагляду веб-хостингу стосувалися веб-сайтів цілком, а не окремих веб-сторінок, **процесуальні вимоги закону не були дотримані**. Не вказавши URL-адреси, органи влади не надали можливості заявникам видалити конкретний незаконний вміст або оскаржити вимогу Генерального прокурора.

Крім того, висновок Генерального прокурора про те, що матеріали на відповідних сайтах становили заклики до участі в несанкціонованих публічних заходах, є **тлумаченням його змісту, яке не мало фактичних підстав, було довільним і явно необґрунтованим**. У приписі щодо www.kasparov.ru також не було жодних правових підстав для тиражування зображення брошури, яка нібито підбурювала людей у Криму до «протиправних дій», однак **генпрокурор не мав законних повноважень щодо визнання, що є незаконним за межами російської юрисдикції**. У будь-якому випадку, **поняття «незаконні дії» вийшло за межі категорій контенту, який підлягає блокуванню відповідно до розділу 15.3**.

<u>Чи було блокування необхідним:</u>

Суд також перевірив, чи було блокування доступу до цілих веб-сайтів у справі цих заявників «необхідним у демократичному суспільстві». Таке комплексне блокування є **крайнім заходом**, який порівнюють із забороною газети чи телевізійної станції, і **вимагає окремого обґрунтування**. Будь-яке **невибіркове блокування, яке втручається в законний контент або веб-сайти як побічний ефект заходів, спрямованих лише на незаконний контент, є свавільним втручанням** у права власників таких веб-сайтів.

<u>Чи були передбачені гарантії проти свавільного втручання:</u>

Заходи блокування, **вжиті до винесення судового рішення про незаконність опублікованого контенту, становили попередні обмеження на публікацій**. Такі обмеження підлягають ретельному судовому аналізу та виправдані лише за виняткових обставин. Особливо це стосується преси, оскільки затримка публікації, навіть на короткий

період, цілком може позбавити усієї цінності та інтересу до ресурсу. У випадках попередніх обмежень на діяльність засобів масової інформації, таких як нинішній, **необхідна законодавча база для забезпечення жорсткого контролю за обсягом заборон і ефективного судового перегляду**.

Російське законодавство не передбачало жодних процесуальних гарантій, зокрема не вимагало будь-якої форми участі власників веб-сайтів у процедурі блокування. І початкове рішення генпрокурора, і виконавчі накази Роскомнагляду були прийняті без попереднього повідомлення зацікавлених сторін. **Закон не вимагав від органів влади проводити оцінку впливу заходів блокування до їх впровадження або обґрунтовувати терміновість їх негайного виконання, надавати зацікавленим сторонам можливість видалити незаконний контент або подати заяву про судовий перегляд. Заходи блокування не були санкціоновані судом чи іншим незалежним судовим органом.**

Більш того, Закон про інформацію не вимагає від органів влади обґрунтовувати необхідність і пропорційність втручання у свободу вираження поглядів в Інтернеті або розглядати питання, чи можна досягти того самого результату за допомогою менш втручальних засобів. Він також не вимагає від них переконатися, що захід блокування суворо націлений на незаконний вміст і не має довільних або надмірних наслідків, у тому числі внаслідок блокування доступу до всього веб-сайту.

Таким чином, було визнано порушення статті 10 Конвенції.

Енгельс проти Росії (Engels v. Russia) (рішення від 23 червня 2020 року)[16]

Факти:

Пан Енгельс – активіст онлайн-свободи в Німеччині. У квітні 2015 року суд зобов'язав місцевого інтернет-провайдера заблокувати доступ до веб-сайту заявника, присвяченого питанням свободи слова та конфіденційності, RosKomSvoboda (www.rublacklist.net), на підставі скарги прокурора. Прокурор стверджував, що інформація про обхід фільтрів контенту, яка була доступна на веб-сайті заявника, повинна бути заборонена до поширення в Росії, оскільки вона дає користувачам доступ до екстремістських матеріалів на іншому, не пов'язаному з цим веб-сайті. Заявник не був поінформований про провадження. Після ухвали суду Роскомнадзор надав вимогу заявникові видалити образливий контент, інакше сайт буде заблоковано. Заявник виконав вимогу та подав скаргу до національного суду, вказуючи, що надання інформації про інструменти та програмне забезпечення для захисту конфіденційності веб-перегляду не суперечить жодному російському законодавству. Суди відхилили скаргу.

Мотивація Суду:

Втручання у права заявника ґрунтувалося на статті 15.1 Закону про інформацію, а саме на другій частині підрозділу 5, яка дозволяла блокувати веб-сайти **на підставі**

[16] https://hudoc.echr.coe.int/eng?i=001-203180

«судового рішення, яке визначало певний інтернет-контент як інформацію, розповсюдження якої повинно бути заборонено в Росії». Суд встановив, що **положення не містить перелік категорій контенту, який підлягає блокуванню, а отже є надто розпливчастим і широким, що не задовольняє вимог Конвенції щодо передбачуваності**. Зокрема, власники веб-сайтів, такі як пан Енгельс, не могли регулювати свою поведінку за допомогою нього, оскільки вони не могли знати, який контент може бути заборонений і призвести до блокування веб-сайту.

Такі законодавчі положення можуть призвести до довільних наслідків. Так, на прикладі пана Енгельса: його веб-сайт було заблоковано, хоча суд не встановив, що інструменти обходу фільтрів та інше програмне забезпечення як таке, чи надання інформації про них, є незаконними. Також суд не знайшов жодних екстремістських висловлювань чи іншого забороненого контенту на веб-сторінці заявника, але послався на можливість того, що технологія може бути використана для доступу до екстремістського контенту в іншому місці. ЄСПЛ зазначив, що приховування інформації про технологію доступу до інформації в Інтернеті, оскільки вона може сприяти доступу до екстремістських матеріалів, нічим не відрізняється від спроби обмежити доступ до принтерів і копіювальних машин, оскільки вони можуть використовуватися для відтворення такого матеріалу. **За відсутності вузько визначеної та конкретної правової основи Суд визнав такий масштабний захід обмеження свавільним**.

Б'янкарді проти Італії (Biancardi v. Italy) (рішення від 25 листопада 2021 року)[17]

Факти:

Заявник був головним редактором інтернет-газети. 29 березня 2008 року він опублікував статтю під назвою ««Бійка в ресторані – начальник поліції закриває ресторани W і Z [які належали фігурантам бійки]». У статті згадувалося рішення керівника поліції закрити ресторани на двадцять днів. У ньому згадувалися імена причетних осіб (двоє братів, V.X. і U.X., і їхні відповідні сини, A.X і B.X.), а також можливий мотив бійки, який, ймовірно, стосувався фінансової сварки щодо права власності на будівлю.

6 вересня 2010 року B.X. і ресторан W надіслав офіційне повідомлення заявнику з проханням видалити статтю з Інтернету, але безуспішно. Далі вони подали позов до суду про вилучення статті з мережі Інтернет та порушення права на повагу до репутації. Заявник заявив, що на той момент стаття була деіндексованою. Національні суди присудили виплату моральної компенсації, оскільки:

- використання персональних даних в статті не відповідало вимогам закону про персональні дані;

[17] https://hudoc.echr.coe.int/fre?i=001-213827

- інформація була легко доступною (більше, ніж будь-яка інформація, опублікована в друкованих газетах, беручи до уваги велике локальне розповсюдження спірної онлайн-газети) шляхом простого введення імен позивачів у пошукову систему;
- характер відповідних даних, що стосується судових проваджень, був чутливим.

Мотивація Суду:

Для цілей рішення Суд визначив термін «деіндексація» для позначення заходу, який заявнику було запропоновано здійснити, щоб гарантувати право V.X. і W на повагу до їх репутації, а саме - видалення зі списку відображених результатів (після пошуку за іменем особи) відповідної Інтернет-сторінки.

Сторони погодилися, що свобода вираження поглядів заявника була порушена рішеннями національних судів і що таке втручання було «передбачено законом». Також наявна законна мета – захистити «репутацію або права інших осіб».

Національні суди не розглядали жодної вимоги щодо остаточного видалення статті. **Заявник несе відповідальність** не за те, що не видалив статтю, а **за те, що не здійснив її деіндексацію** (дозволяючи протягом надмірного періоду демонструвати інформацію про кримінальне провадження після введення в пошуковій системі назви ресторанів або V.X.).

Важливими ознаками даної справи є **(1) період, протягом якого онлайн-стаття залишалася в Інтернеті**, і вплив цього на право відповідної особи на повагу до її репутації; **(2) характер відповідного суб'єкта даних** – тобто приватної особи, яка не діє в публічному контексті як політичний чи громадський діяч.

У першому аспекті Суд відмітив, що хоча кримінальне провадження, про яке йшлося в статті досі тривало, однак інформація в статті про нього не оновлювалася. Стаття лишалася легкодоступною протягом восьми місяців, хоча **актуальність права заявника на поширення інформації зменшилася з плином часу порівняно з правом V.X. на повагу до його репутації**.

Крім того, Суд вважає, що суворість вироку та розмір компенсації, призначеної у зв'язку з відшкодуванням моральної шкоди (5000 євро кожному позивачу), не можна вважати надмірною з огляду на обставини цієї справи.

Відповідно, порушення статті 10 Конвенції не було.

D. Аналіз застосовних міжнародних інструментів та практики Європейського суду з прав людини.

Загальний огляд міжнародних та іноземних підходів

За загальним правилом на міжнародному рівні та в іноземних країнах, блокування вебресурсів (web-blocking) розглядається як крайній захід, який у випадку

необґрунтованості може розглядатися як вияв державної чи приватної цензури[18]. Водночас, у деяких випадках та за умови дотримання певних стандартів, в тому числі для поваги до прав і свобод третіх осіб, застосування веб-блокування розглядається як допустимий і, навіть, необхідний крок[19].

Такими випадками найчастіше виступають:

1. Порушення авторських прав: неліцензоване поширення за допомогою вебресурсів інформації, яка є результатом творчої роботи автора або групи авторів;
2. Захист прав та інтересів неповнолітніх осіб (протидія поширенню дитячої порнографії та ін.);
3. Поширення інформації, яка розпалює ненависть та провокує агресію та ін.[20]

Хоча порушення приватності, в тому числі, у формі поширення великих обсягів персональних даних, розглядаються в одному ряду із іншими кіберзлочинами[21], однак найчастіше не розглядається як пріоритетна мета веб-блокування. Тим не менше, з вступом дію Загального Регламенту ЄС щодо захисту персональних даних (GDPR), це питання активізувалося, наприклад Бельгія запровадила спеціальну процедуру блокування вебресурсів у зв'язку із порушенням приватності. У Великобританії, в новому законодавстві про онлайнбезпеку, хоча порушення приватності як фактична підстава для блокування випливає зі змісту закону.

Аналіз актів міжнародних організацій та рішень міжнародних судових органів, дозволяє виокремити низку стандартів, які повинні застосовуватися при прийнятті рішень про блокування вебресурсів або ж впровадженні відповідних процедур:

- блокування вебресурсів розглядається як крайній захід, необхідний для припинення правопорушення, який має застосовуватися у спосіб, який допускатиме вжиття свавільних заходів і не створюватиме «охолоджувального ефекту» в подальшому[22];

---

[18] Див. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society (CM(2005)56 final of 13 May 2005) «обмежений доступ або відсутність доступу до [інформаційно-комунікаційних технологій (ІКТ)»] може позбавити людей можливості повною мірою реалізовувати свої права... ІКТ також створюють багато серйозних проблем для цієї свободи [вираження поглядов], наприклад, державна та приватна цензура».

[19] Див. its General Comment No. 34 on Article 19 of the International Covenant on Civil and Political Rights, adopted at its 102nd session (11 29 July 2011) « Будь-які обмеження на роботу веб-сайтів, блогів або будь-якої іншої електронної або іншої системи розповсюдження інформації в Інтернеті ..., допустимі лише в тій мірі, в якій вони сумісні з параграфом 3 (ст. 19 Міжнародного пакту про громадянські та політичні права).

[20] Див. Report by the Organization for Security and Co-operation in Europe (OSCE) entitled "Freedom of expression on the Internet: study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States" «введені спеціальні законодавчі положення, які дозволяють блокувати доступ у разі певних видів правопорушень. До них належать дитяча порнографія, расизм, мова ворожнечі, підбурювання до тероризму та наклеп».

[21] Див. The Convention on Cybercrime (ETS No. 185 which came into force on 1 July 2004) «дії, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем».

[22] Див. Recommendation 2008/2160(INI), adopted by the European Parliament on 26 March 2009 «забезпечити, щоб свобода вираження поглядів не підлягала свавільним обмеженням з боку публічної та/або приватної

- блокуванню має передувати вимога (адміністративна чи судова) про припинення правопорушення[23];
- такий захід має носити спершу тимчасовий і, лише згодом, після ухвалення остаточного судового рішення або небажання чи неможливості усунути проблему – постійний характер;
- при здійсненні блокування має бути врахований принцип пропорційності – застосований захід має, за можливості, бути спрямований на конкретний контент, а не на вебресурс в цілому[24];
- при прийнятті рішення про блокування і його здійснення слід враховувати зміст спеціальних правових актів, які регламентують ту чи іншу сферу (наприклад, у випадку блокування через поширення персональних даних в ЄС – GDPR)[25];
- зазначені стандарти мають бути дотримані як публічними, так і приватними суб'єктами, які застосовують чи можуть застосовувати відповідні заходи.

Важливим аспектом також є спосіб ухвалення рішення – адміністративний чи судовий. Загальним стандартом є те, що такі рішення мають прийматися, як правило, саме в судовому порядку, особливо коли мова йде про блокування ресурсу на постійній основі, що підтверджується і практикою Конституційної ради Франції[26]. Водночас, тимчасові обмеження здійснені на підставі адміністративних рішень можуть розглядатися як допустимі, за умови можливості судового оскарження, а блокування на постійній основі – лише згідно з рішенням суду.

В той же час презюмується, що суд, в межах своєї дискреції, може ухвалювати відповідні рішення самостійно, навіть без наявності спеціальної процедури, передбаченної законодавством. Однак вимоги щодо пропорційності, необхідності та мети, яка полягає у захисті законних прав та інтересів є незмінними.

Чи не найкраще зарубіжні практики в цій сфері ілюструють національні практики Великобританії та Бельгії.

сфери та уникати всіх законодавчих чи адміністративних заходів, які можуть мати «охолоджувальний ефект» на всі аспекти свободи слова»

[23] Див. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society (CM(2005)56 final of 13 May 2005) «За умови дотримання гарантій пункту 2 статті 10 Конвенції про захист прав людини та основоположних свобод можуть бути вжиті заходи для примусового видалення чітко ідентифікованого Інтернет-контенту або, альтернативно, блокування доступу до нього, якщо компетентні національні органи прийняли тимчасове або остаточне рішення про його незаконність».

[24] Див. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society (CM(2005)56 final of 13 May 2005) «Такі заходи, які можуть передбачати певний вид попереднього контролю, повинні відповідати вимогам пункту 2 статті 10 Конвенції про захист прав людини та основоположних свобод, і вони повинні бути спрямовані на чітко ідентифікований Інтернет-контент».

[25] Див. Case of Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (Court of Justice of the European Union) «національні правила мали дотримуватися обмежень, що випливають із законодавства Європейського Союзу, зокрема з Директиви про електронну комерцію (2000/31/EC)»

[26] Див. Decision of 10 June 2009 (no. 2009-58 DC) of the French Constitutional Council « розпорядження про призупинення доступу може бути видане лише після змагального судового провадження як додаткове покарання»

Практика Великобританії

У Великобританії питанню захисту персональних даних історично приділяється значна вага і власне концепт "приватність" (privacy) зародився саме там. Хоча Британія і вийшла із Європейського Союзу внаслідок "Брекзиту", там у 2018 році було розроблено і прийнято Акт про захист даних (Data Protection Act)[27], який є повністю сумісним із GDPR, дія якого поширюється, в тому числі, на захист приватності в Інтернеті.

До інституційного механізму захисту приватності в Інтернеті належать у першу чергу, Інформаційний комісар та його Офіс (Information Commissionner's Office), які є уповноваженим органом в сфері захисту персональних даних. З іншого боку, відповідними компетенціями наділений і урядовий Офіс з питань комунікацій (Office of Communications (Ofcom), до функцій якого належить запобігання порушенням приватності в Інтернеті і, який працює безпосередньо із Інтернет-провайдерами (Internet Service Providers, ISPs).

Безпосередньо блокування здійснюють компанії, які є Інтернет-провайдерами (Internet Service Providers, ISPs). Інтернет-провайдери отримують сповіщення з вимогою про блокування певних веб-сайтів або певного вмісту і впроваджують блокування за допомогою блокування DNS, блокування IP-адрес або фільтрації URL-адрес. В подальшому, провайдери можуть перевірятися на предмет виконання ухвали суду чи адімінстративного рішення, і від них може вимагатися звітувати про їх виконання.

У жовтні 2023 року було прийнято Закон про онлайнбезпеку (Online Safety Act)[28], який, в тому числі, регламентує повноваження Ofcom із блокування сайтів у зв'язку із порушенням приватності. Передбачається, що ці важелі слід застосовувати у випадках, коли недотримання вимог створює справжній і серйозний ризик завдати істотної шкоди особам у Великобританії.

Положення Online Safety Act встановлюють, якщо до онлайн-ресурсу є зауваження, в тому числі в частині поширення персональних даних, Ofcom може звернутися до суду за наказом про тимчасове/постійне ***обмеження обслуговування*** таких ресурсів. Однак фактично, метою розпорядження є не застосувати санкцію до ресурсу чи сервісу - порушника, а обмежити здатність надавати її: такі вимоги можуть застосовуватися до платіжних систем та рекламних сервісів, пошукових систем, які індексують сервіс, і різні користувацьких програм, які дозволяються отримувати доступ до нього, в тому числі – і до провайдерів хостингу. Своєю чергою це призводить до неможливості функціонування сервісу чи ресурсу, в т.ч. його блокування.

Окрім того, Ofcom може звернутися до суду з клопотанням про тимчасове/постійне ***обмеження доступу*** до ресурсу, який або не здатний захистити користувачів Великобританії від значної шкоди, або вже заподіяв її. Наказ про обмеження доступу означає, що постачальники послуг Інтернету повинні заблокувати особам у Великобританії можливість доступу до відповідного ресурсу. Наказ про обмеження доступу також можуть

[27] Див. https://www.gov.uk/data-protection
[28] Див. https://www.legislation.gov.uk/ukpga/2023/50/enacted

також вимагати від магазинів застосунків (AppStore, Google Play та ін.) зупинити можливість завантажувати застосунок у Великобританії.

Згідно з Online Safety Act, Ofcom повинен оприлюднювати заходи примусу, які вони вживають, включно із блокуванням ресурсів. Однак допускається, що OFCOM може не публікувати цю інформацію, якщо вона є комерційно чутливою або є інші приводи робити її конфіденційною.

Практика Бельгії

Наприкінці 2021 року, бельгійський органі із захисту персональних даних (L'Autorité de protection des données veille, APDV) уклав меморандум із DNS Belgium – некомерційною організацією, що управляє доменними іменами в Бельгії. Ним було врегульовано право APDV вимагати закриття веб-сайтів в домені .be, в тому разі, якщо вони порушують GDPR[29].

Згідно з Протоколом Інспекція та Судова палата APDV можуть використовувати цю так звану «Процедуру сповіщення та дій» як доповнення до своїх існуючих повноважень щодо припинення, обмеження, заморожування або припинення діяльності з обробки даних, у разі «серйозної та безпосередньої шкоди, яку важко усунути». Це рішення є тимчасовим заходом до прийняття рішення по суті Судової палати.

Ця процедура може бути розпочата тоді, коли Інспекція або Судова палата наказали контролеру чи обробнику призупинити, обмежити, заморозити чи припинити діяльність з обробки даних, яка вважається незаконною. І якщо контролер або процесор не виконав цей наказ у встановлений термін, APDV може надіслати повідомлення DNS Belgium, щоб ініціювати процедуру повідомлення та дії.

Після отримання такого повідомлення DNS Belgium здійснить наступні дії протягом 1 робочого дня:

- повідомляє контролера або процесора про повідомлення APDV;
- перенаправлятиме користувачів із підсанкційного спірного доменне імені на сторінку із попередженням APDV, тим самим заблокувавши відповідний веб-сайт.

Після повідомлення контролер або процесор отримує 14-денний періоду для усунення проблеми, який може бути продовжений APDV. Якщо ж порушення протягом цього періоду не будуть усунені, DNS Belgium збереже перенаправлення протягом додаткового періоду 6 місяців, після чого скасує реєстрацію доменного імені в цілому.

DNS Belgium наголошували, що ця процедура буде використовуватися тільки як крайній захід в тих випадках, коли порушення GDPR завдають особливо великої шкоди інтересам суб'єктів даних і коли вони свідомо здійснюються.

Після повідомлення про блокування, контролер або процесор має кілька варіантів дій.

[29] Див. https://www.admeet.eu/en/protocol-dns-apd/

По перше він може усунути порушення протягом 14 днів. У цьому випадку DNS Belgium скасує перенаправлення, внаслідок чого веб-сайт знову стане доступним.

У випадках, коли контролер або процесор не погоджується з рішенням, він також повинен мати право оскаржити це рішення. Хоча у Протоколі це питання прямо не врегульоване, презюмується, що буде застосовуватися звичайна процедура апеляції в комерційному суді, як існує у випадку інших рішень APDV.

Якщо власник доменного імені може довести, що кваліфікація APDV є помилкою, яка завдала йому шкоди, він може притягнути APDV до відповідальності відповідно до цивільного законодавства та виплатити компенсацію шкоди, заподіяної з її «вини». Цікаво, що у французькій версії протоколу в цьому пункті використовується термін "erreur", а не "faute", який можна інтерпретувати як "помилку", що, мабуть, є ширшим поняттям, ніж "вина" відповідно до бельгійського цивільного законодавства.

По-перше, існує проблема, пов'язана з правом на захист у випадках, коли APDV не заслухавши відповідача, а саме APDV, у цьому випадку, діятиме як прокурор та суддя водночас.

По-друге, сумнівно, не зрозуміло як скорелювати остаточне анулювання реєстрації доменного імені, з тим фактом, що APDV має право вживати лише тимчасових заходів, які не можуть перевищувати шести місяців.

По-третє те, що DNS Belgium заблокує веб-сайт одночасно з повідомленням контролера або оброблювача, передбачає, що потенційна апеляція, не запобіжить закриття веб-сайту.

По-четверта, поріг доказування вини та умови, які мають бути дотримані, чітко не визначені та відкриті для довільного трактування.

Згодом було уточнено, що ця процедура буде застосовуватися лише в тому випадку, якщо «всупереч офіційній вказівці APDV, веб-сайт продовжуватиме обробляти персональні дані».

При цьому DNS Belgium вказувало, що має бути чіткий зв'язок між веб-сайтом або доменним ім'ям та фактом порушення приватності.

Висновки

Слід констатувати, що блокування Інтернет ресурсів зазвичай розцінюватиметься в якості втручанням в право на свободу вираження поглядів, гарантоване зокрема ст. 10 Конвенції. Сам по собі такий захід не забороняється практикою ЄСПЛ чи іншими міжнародними документами. Однак, він повинен здійснюватися з дотриманням передбачених ними вимог. Йдеться, серед іншого і про ч. 2 ст. 10 Конвенції та відповідну практику ЄСПЛ.

Будь-яке блокування Інтернет-ресурсів, відтак, повинно бути законним, переслідувати одну з прийнятних в демократичному суспільстві легітимних цілей, та бути необхідним.

Легітимними цілями у такій категорії справ традиційно можуть вважатись захист авторських прав, боротьба з поширенням дитячої порнографії, мови ненависті, расистських поглядів та ідей, закликів до вчинення терористичних актів, висловлювань, що принижують честь, гідність, ділову репутацію та інше.

Обмеження доступу до Інтернет-ресурсів повинно ґрунтуватись на чітких законодавчих підставах, мати чітко визначені межі та супроводжуватись ефективним судовим контролем. Законодавство повинно чітко визначати категорії інформації, доступ до якої підлягає блокуванню, а також межі повноважень контролюючого органу. Такий орган не повинен володіти необмеженою дискрецією в реалізації вказаних повноважень. Він повинен вжити розумних заходів з метою попереднього влагодження проблеми, наприклад: попередити власника (адміністратора) веб-ресурсу про незаконність поширення певної інформації та надати йому можливість самостійно її видалити. Таке попередження (чи вимога щодо видалення) повинна містити чітке посилання на конкретну інформацію чи URL-адресу, яка порушує законодавчі вимоги. Лише невиконання такої вимоги чи відсутність реагування може стати підставою для прийняття рішення щодо блокування. Будь-яке рішення такого характеру повинно містити посилання на передбачені законодавством підстави, та відповідне обґрунтування щодо їх наявності у даній справі.

Рішення про блокування Інтернет ресурсу може прийматись адміністративним органом, однак повинно бути предметом ретельного судового контролю. Поширена інформація може втрачати свою цінність з часом, відтак судовий перегляд повинен бути також швидким. В ідеалі рішення щодо блокування повинне бути санкціоноване судом чи іншим незалежним судовим органом. Власнику (адміністратору) веб-ресурсу необхідно надати можливість представити свою позицію в суді. Зокрема, він повинен з урахуванням терміновості питання мати належні час та можливості для підготовки своєї позиції по справі.

Блокування цілого веб-сайту є більш жорстким заходом, що за своєю суттю можна прирівняти до заборони газети чи телевізійної станції, і вимагає більш вагомого обґрунтування. Будь-які обмеження на інтернет ресурси повинні бути спрямовані проти конкретної інформації (публікації, фото- чи відеозображення) чи URL-адреси. Загальні заборони на функціонування певних веб-ресурсів та систем є крайніми і загалом не бажаними заходами. В будь-якому випадку не можна блокувати доступ до цілого веб-сайту лише з огляду на зміст однієї сторінки такого ресурсу чи розміщеної на ньому публікації.

Рішення щодо блокування інформації повинне містити обґрунтування щодо необхідності і пропорційності втручання у свободу вираження поглядів в Інтернеті, зокрема, містити аналіз щодо того, чи можна досягти того самого результату за допомогою менш інтрузивних засобів. Орган влади, що виносить відповідне рішення повинен переконатись, що захід блокування націлений лише на незаконний вміст і не має довільних або надмірних наслідків, зокрема проаналізувати, чи не зачіпає він права третіх осіб. Такі вимоги до рішення про блокування необхідно закріпити у законодавстві.

Незаконне блокування веб-ресурсів повинно бути підставою для відшкодування збитків, завданих власнику ресурсу.

Не допускаються обмеження інформації політичного характеру з тих лише міркувань, що вона містить критику чинної влади чи політичної системи.

У випадку поширення інформації щодо приватного життя особи, зокрема чутливих персональних даних чи надмірної кількості персональних даних або інформації, що порочить честь, гідність та ділову репутацію особи, вагомим фактором є швидкість реагування на такий інцидент. Чим довше така інформація перебуває у вільному доступі, тим більшої шкоди може бути завдано особі.

У підсумку:

1. Блокування інтернет ресурсів з метою недопущення поширення чутливих категорій персональних даних, надмірних обсягів персональних даних чи інформації, що порочить честь гідність чи ділову репутацію **є допустимим заходом.**
2. Орган, який здійснює контроль за додержанням законодавства про захист персональних даних може бути наділений повноваженнями звернення до суду із позовом пор блокування інтернет ресурсу.
3. Зверненню до суду повинна передувати комунікація і власником (адміністратором) веб-ресурсу з метою змусити його самостійно видалити відповідну інформацію.
4. Орган, який здійснює контроль за додержанням законодавства про захист персональних та суд повинні вжити розумних заходів для того, щоб забезпечити участь власника (адміністратора) веб-ресурсу у судовому розгляді.
5. Як власник (адміністратор), так і треті особи, чиї права обмежено рішенням суду, повинні володіти правом на його оскарження.
6. Як процедура розгляду позову, такі і судове рішення повинні відповідати переліченим вище вимогам.
7. Рекомендується підійти до питання блокування веб-ресурсів більш комплексно та розглянути можливість усунення прогалин та недоліків в чинному законодавстві, що регламентує питання блокування веб-ресурсів, а саме:
    - Чітко врегулювати діяльність у цій сфері Національного центру оперативно-технічного управління електронними комунікаційними мережами України;
    - Забезпечити процедуру накладення санкцій, яка б супроводжувалась достатніми гарантіями захисту прав осіб, чиї права було обмежено шляхом блокування веб-ресурсу;
    - Врегулювати процес роботи системи боротьби з фішинговими веб-сайтами на рівні законодавства та запровадити механізми захисту прав потерпілих.
8. Рекомендується запровадити єдиний підхід до системи блокування веб-ресурсів в Україні.

Summary

The research aimed to assess Ukrainian legislation regarding the blocking of web resources with a focus made on privacy protection and preventing personal data leaks to ensure compliance with the European Convention on Human Rights and the best international practices. The assessment revealed that the current legislation is confusing, unclear, and contains numerous institutional inconsistencies. It lacks provisions for independent oversight and remains opaque to the public and stakeholders.

Additionally, the legislation lacks specific provisions for blocking web resources to protect privacy, combat hate speech, and safeguard intellectual property rights. It has been concluded that new legislation is needed, one that outlines clear and consistent procedures for decision-making on blocking, appeals, and democratic control of such decisions. This legislation should include specific rules for blocking web resources for various reasons, including protecting privacy, copyright, and the rights and interests of children, among others.

This legislation should be founded on the principles of legality, proportionality, and necessity, to protect privacy and prevent the dissemination of sensitive information. Blocking should only be considered a last resort, preceded by efforts to compel the resource owner to remove unacceptable content. Any decision to block must be justified, striking a balance between the right to freedom of speech (Article 10 of the Convention) and the right to privacy (Article 8 of the Convention), with the provision for judicial appeal.

These measures must be proportionate, targeting only the part of the web resource that violates standards, rather than the entire website. Informing the resource owner about the blocking process is crucial for ensuring transparency and fairness, thereby safeguarding their rights as well as those of third parties involved in the decision-making process.

Effective blocking implementation requires synchronized efforts among data protection, information security, and internet administration authorities. The goal of legislative improvements is to streamline the blocking process, uphold human rights, and regulate efforts against phishing, while avoiding excessive or arbitrary blocks.