

ЛІТЕРАТУРА:

1. Конституція України. Відомості Верховної Ради України (ВВР). 1996. № 30. с. 141. URL: <http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>.
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України (ВВР). 2010. № 34. ст. 481. URL: <http://zakon5.rada.gov.ua/laws/show/2297-17>.

*Ващак Владислав Анатолійович,
аспірант кафедри цивільного права
Національного університету «Одеська юридична академія»*

КІБЕРВОЄННИЙ СТАН В УКРАЇНІ: ОБМЕЖЕННЯ ПРАВА НА ДОСТУП ДО ІНТЕРНЕТУ В УМОВАХ ВОЄННОГО СТАНУ

З початком введення воєнного стану в Україні 24 лютого 2022 року ряд прав та свобод українців було обмежено для гарантування захисту та обороноздатності країни. В умовах війни протистояння поширюється і на інтернет-сферу. Так, онлайн-середовище використовується для поширення дезінформації, стеження за переміщенням військових, місцем розташування об'єктів військової та критично важливої інфраструктури. В таких умовах державою запроваджується ряд обмежень для цілей національної безпеки та унеможливлення зловживанням правом на доступ до інтернету.

Кібервоєнним станом можна назвати усі заходи, введені державною владою, які перешкоджають доступу до інформації або її поширенню в Інтернеті, також контролюють та використовують Інтернет для забезпечення загального блага та обороноздатності країни, національної безпеки. Вони можуть набувати різних форм, зокрема: обмеження пропускнуої здатності, що спричиняє низьку швидкість Інтернету, яка дозволяє завантажувати лише текст, блокування певних веб-ресурсів, таких як соціальні мережі або служби обміну повідомленнями, а також часткове або повне відключення доступу до Інтернету. [1].

Нині Інтернет став одним із основних засобів реалізації права на свободу отримання та поширення інформації та ідей, що забезпечує

необхідними інструментами для участі в діяльності та дискусіях з політичних питань та питань, що становлять загальний інтерес. Більше того, що стосується важливості Інтернету у здійсненні свободи вираження поглядів, то його доступність і здатність зберігати та передавати величезні обсяги інформації, відіграє важливу роль у реалізації громадськості доступу до новин і сприяння поширенню інформації в цілому. Створена користувачами діяльність в Інтернеті забезпечує безпрецедентну платформу для здійснення свободи вираження поглядів...» (Cengiz та інші проти Туреччини, рішення ЄСПЛ від 1 грудня 2015 року, §§ 49 і 52) [2].

Варто зазначити, що міжнародне законодавство, незважаючи на важливість права на свободу слова, в тому числі і в Інтернеті може встановлювати обмеження щодо реалізації такого права. Так, Європейська конвенція з прав людини в ч. 2, ст. 10 зазначає, що «Здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду» [3].

В умовах кібервоєнного стану інтернет-технології повинні використовуватися для досягнення загальнодержавних цілей (подолання агресії, фіксування злочинів і т.д.). Цифрові технології є потужними інструментами для збору доказів. В умовах кібератак та збоїв в Інтернеті люди в Україні за підтримки Міністерства цифрових технологій працюють над документуванням і каталогізацією злочинів, скоєних російськими військами, за допомогою чат-ботів, додатків і веб-сайтів.

З початку вторгнення українські чиновники, юристи та правозахисні групи намагаються розробити нові способи каталогізації та перевірки численних відео, фотографій та свідчень очевидців злочинної поведінки російських військ. Варто зауважити, що компанії, які адмініструють соціальні медіа, повинні відкоригувати свою політику модерації контенту, щоб зберегти матеріал з доказовою цінністю та гарантувати, що облікові записи очевидців не будуть заблоковані за поширення вмісту з елементами насильства. Платформи соціальних

мереж зобов'язані забезпечити людям доступ до вільного доступу до збереження інформації в Україні та в інших кризових зонах по всьому світу [4].

Світ, як фізичний, так і цифровий, опиняється в безпрецедентному часі, в умовах війни в Україні. Корпоративні гіганти, такі як Meta, Google і Apple, які завжди вважали себе нейтральними технологічними фірмами, тепер розміщують кольори прапору України, на своїх веб-сайтах, забороняють реалізацію своїх продуктів у Росії у відповідь на її вторгнення. Тим часом, сам Інтернет змінюється для російських користувачів – заблоковані Twitter і Facebook, TikTok не дозволяють російським користувачам публікувати повідомлення, а поліція, як повідомляється, зупиняє людей на вулицях, щоб подивитися, що вони переглядають на своїх телефонах [5].

Отже, у підсумку можна зазначити, що введення особливого правового режиму використання Інтернету (кібервоєнного стану) є важливим інструментом для забезпечення національної безпеки в кризових ситуаціях. Так, в демократичному суспільстві ми не говоримо про повне відключення доступу до мережі, а скоріше його контролюваність та специфічне використання.

ЛІТЕРАТУРА:

1. Internet shutdowns and human rights. URL: <https://www.ohchr.org/sites/default/files/Documents/Press/Internet-shutdowns-and-human-rights.pdf>
2. Access to Internet and freedom to receive and impart information and ideas. URL: https://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf
3. Конвенція про захист прав людини і основоположних свобод (з протоколами) URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
4. Updates: Digital rights in the Russia-Ukraine conflict URL: <https://www.accessnow.org/digital-rights-ukraine-russia-conflict/>
5. Russia-Ukraine: Is internet on verge of break-up? – BBC News URL: <https://www.bbc.com/news/technology-60661987>