

МОНІТОРИНГ ПОРУШЕНЬ ЦИФРОВИХ ПРАВ В УКРАЇНІ

Аналітичний звіт

Період моніторингу – липень 2019 року

I. Порухення цифрових прав загального характеру (порушення, які мають вплив на необмежене коло осіб).

1. Доступ до Інтернету.

- 1) В липні 2019 року продовжувалось блокування 240 веб-сайтів на підставі двох Указів Президента України від 15 травня 2017 року¹ та від 14 травня 2018 року², що вже відмічалось у попередніх аналітичних звітах за результатами Моніторингу порушень цифрових прав в Україні³. Порухення носить триваючий характер і жодних покращень ситуації у липні 2019 року не відбулось.
- 2) У липні 2019 в Єдиному державному реєстрі судових рішень оприлюднено постанову Великої Палати Верховного Суду від 05.06.2019 у справі № П/800/217/17 за позовом ГО «Автономна адвокатура» до Президента України Порошенка Петра Олексійовича про визнання частково незаконним і скасування указу від 15 травня 2017 року № 133/2017 «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»⁴. Цим рішенням Суд визнав перший Указ Президента законним, таким що має легітимну мету (загроза національним інтересам та безпеці України), є необхідним у демократичному суспільстві. Нагальна потреба у такому рішенні обгрунтована виключно фактом агресії Російської Федерації проти України. Інші критерії балансування прав не застосовувались (зокрема, не оцінювалась пропорційність такого кроку, його наслідки тощо).

Велика Палата Верховного Суду також зазначила, що позивач не був позбавлений можливості використовувати для одержання, зберігання та передачі інформації інші веб-ресурси, аналогічні до тих, доступ до яких було обмежено оскаржуваним Указом, у зв'язку з чим дійшла висновку про відсутність порушень прав позивача.

Зважаючи на це, хочемо нагадати, що Коаліцією «За вільний Інтернет» було підготовлено і опубліковано юридичний аналіз Указу Президента України 2018-го року, висновки якого, в переважній більшості, є релевантними і до першого Указу⁵.

Серед основних:

¹ <https://www.president.gov.ua/documents/1332017-21850>

² <https://www.president.gov.ua/documents/1262018-24150>

³ <https://www.ppl.org.ua/monitoring/monitoring-cifrovix-prav>

⁴ <http://www.reyestr.court.gov.ua/Review/82738705>

⁵ <https://www.ppl.org.ua/yuridichnij-analiz-ukazu-prezidenta-pro-blokuvannya-sajtiv.html>

- санкція, як спосіб обмеження прав і свобод людини не відповідає конституційним стандартам і вимогам і є проявом необмеженої дискреції державної влади;
- секторальний характер санкції для введення в дію потребує позитивного голосування у Верховній Раді України;
- механізм в частині блокування сайтів не відповідає національному законодавству та порушує основні конституційні права громадян;
- практика блокування сотень веб-сайтів в спосіб, який застосовано владою, не відповідає критерію «передбачено законом» в розумінні міжнародно-правових договорів та практики Європейського суду з прав людини;
- таке блокування не відповідає критерію «необхідності в демократичному суспільстві», є непропорційним визначеній законній меті.

2. Інтернет і виборчий процес.

- 1) У липні 2018 в Єдиному державному реєстрі судових рішень опубліковано **3 (три)** рішення у справах про порушення обмежень щодо ведення передвиборної агітації:
 - Одна із цих справ стосується оприлюднення користувачем соціальної мережі «Фейсбук» фотографії свого бюлетеня із результатами голосування в день голосування під час проведення голосування⁶.

Проте, встановивши зазначений факт, суд не побачив порушення закону. Він зробив висновок, що фотографування та демонстрація свого бюлетеня, за яким особа здійснювала голосування, поза межами приміщення для голосування не є порушенням таємниці голосування згідно [Закону України «Про вибори Президента України»](#). Питання про порушення обмежень щодо проведення передвиборної агітації (агітація поза строками) судом **не розглянуто**.

Отже, моніторинг показує, що практика оприлюднення результатів голосування в день голосування у соціальній мережі Фейсбук набуває популярності. Такі дії становлять явне порушення встановлених законом обмежень щодо строків проведення агітації (агітація в день виборів заборонена). Водночас, судова практика стосовно окресленої проблеми є неадекватною і не сприяє її вирішенню, що ми вже відмічали і у попередніх звітах. Такий стан речей не дозволяє забезпечити рівні умови участі у виборчих перегонах для усіх кандидатів.

- Інші **дві справи** стосуються поширення матеріалів передвиборної агітації в мережі Фейсбук особами, яким це заборонено законом (заступником міського голови та членом ОВК)⁷. В обох випадках суди не встановили порушень виборчого законодавства, хоча встановили факти поширення матеріалів передвиборної агітації на особистих сторінках зазначених осіб у Фейсбуці.

В одній справі суд взяв до уваги пояснення про те, що мав місце злам персональної сторінки користувачки, а в іншій - дійшов неочікуваного висновку про те, що “фактичні дії відповідача з репосту (опублікування) на своїй сторінці у соціальній мережі «Фейсбук», яка не є електронним засобом масової інформації, **не є поширенням** агітаційних матеріалів як серед своїх друзів, так і серед необмеженого кола осіб”, оскільки “не володіючи назвою профілю відповідача в соціальній мережі «Фейсбук» пересічний громадянин не зможе отримати вказану інформацію”.

⁶ <http://www.reyestr.court.gov.ua/Review/83222658>

⁷ <http://www.reyestr.court.gov.ua/Review/83267285> та <http://www.reyestr.court.gov.ua/Review/82998235>

Така позиція суду суперечить роз'ясненням Пленуму Верховного Суду України,⁸сталій судовій практиці щодо поширення інформації в Інтернеті та сучасним реаліям. В контексті цього дослідження ми мусимо зауважити, що належна практика протидії порушенням виборчого законодавства судами не формується, що несе загрози для реалізації права на вільні вибори.

- 2) Порушення засобами масової інформації правил інформування та проведення передвиборної агітації під час виборів. Зокрема, відповідно до повідомлень деяких медіа, низка рівненських ЗМІ оприлюднювала так звані результати соціопитувань, які, не містили необхідної інформації, передбаченої законом, і мали ознаки недостовірності та маніпулятивності, а також замовності на користь окремих політиків. Така інформація поширювалась в тому числі за допомогою веб-сайтів⁹.
- 3) Створення фейкової сторінки КМІСу, на якій оприлюднювалась інформація про дослідження в різних округах¹⁰.
- 4) Створення фейкового аккаунту одного з кандидатів у народні депутати через який поширювалась інформація, що має ознаки підкупу виборців¹¹.

II. Порушення цифрових прав індивідуального характеру (порушення, які стосуються окремих осіб і не мають безпосереднього впливу на широку аудиторію).

1. Факти порушення прав на свободу вираження поглядів:

- 1) Блокування **19 веб-сайтів** на підставі ухвали суду. Так, 23.07.2019 ухвалою Печерського районного суду м. Києва в рамках кримінальної справи № 757/38387/19-к про накладення арешту на майнові права інтелектуальної власності, які виникають у користувачів мережі Інтернет при використанні 19 веб-сайтів, зобов'язано низку великих українських Інтернет-провайдерів закрити до них доступ¹².
- 2) Блокування Фейсбуком сторінки меморіального проекту "Книга пам'яті полеглих за Україну"¹³.
- 3) DDoS-атаки на портал Delo.ua, що призвело до того, що зазначений веб-ресурс міг бути недоступним протягом кількох днів¹⁴.
- 4) Спам-розсилка вірусних файлів від імені Державної фіскальної служби, яка виявила, що від її імені розсилаються листи про наявність податкового боргу, що містять вкладення, відкриття яких призводить до завантаження вірусного файлу¹⁵.

⁸ https://zakon.rada.gov.ua/laws/show/v_001700-09#o44

⁹ https://4vlada.com/na-redaktorku-rivnenskogo-zmi-sklaly-protokol-cherez-poshyrennia-falshyvogo-rejtyngu?fbclid=IwAR2ufic6Xmy62H7xYNrrk4tvNoolE_DH_1sm8WIFw_DABmfAbwkBjEFb1Y8

¹⁰ <http://kiis.com.ua/?lang=ukr&cat=news&id=870&page=1,>
https://ms.detector.media/ethics/manipulation/u_feysbutsi_stvorili_feykovu_storinka_kmis_scho_publicue_falshivu_sotsiologiyu/

¹¹ <https://netfreedom.org.ua/pokazhy-pasport-nagodyuyut-v-restorani-yak-dezinformatsiya-na-vyborah-poshyryuyetsya-v-sotsmerezah/>

¹² <https://www.facebook.com/cyberlabUkraine/photos/a.1573858602657653/2445565675486937/?type=3&theater>

¹³ <https://www.pravda.com.ua/news/2019/07/14/7220885/>

¹⁴ <https://detector.media/infospace/article/169347/2019-07-26-sait-deloua-zaznav-ddos-ataki/>

¹⁵ <https://www.facebook.com/SFSofUkraine/photos/a.822504774450181/2625309500836357/?type=3&theater>

- 5) Блокування сайту “Український тиждень” німецьким провайдером Hetzner Online GmbH на вимогу Роскомнагляду.¹⁶

2. Приватне життя та захист даних:

- 1) один із депутатів Черкаської міської ради VIII скликання, за депутатським запитом отримав від Черкаської міської ради Будівельний паспорт одного з об'єктів будівництва певної громадянки, який містив її персональні дані і виклав його у вільному доступі на веб-сторінці в соціальній мережі «Фейсбук». Це призвело до незаконного доступу до них невстановленого кола осіб та безпідставного втручання у її приватне життя. Постановою Соснівського районного суду м. Черкаси від 04.07.2019 його притягнуто до адміністративної відповідальності і стягнуто штраф у розмірі 3400 грн¹⁷.

Проте питання про видалення цієї інформації не вирішувалось і не може бути вирішеним в межах провадження у справах про адміністративні правопорушення. Це в свою чергу піднімає питання про ефективність способів правового захисту права на приватне життя (захист персональних даних) в Україні.

- 2) неналежне зберігання відеозапису, зробленого поліцейськими під час проведення превентивних заходів, внаслідок чого це відео оприлюднено сторонньою особою в мережі Фейсбук та відмова адміністративних судів захистити право на захист персональних даних позивача.

Так, постановою Третього апеляційного адміністративного суду від 09.07.2019¹⁸ відмовлено в розгляді в порядку адміністративного судочинства позову, в якому ставилось питання про визнання зазначених дій та бездіяльності поліцейських протиправними. Суди першої та апеляційної інстанцій дійшли висновку про те, що ця справа не підсудна адміністративним судам, а підняте питання повинно розглядатись в порядку кримінального судочинства.

Проте, такий підхід робить захист персональних даних особи неефективним, хоча б з огляду на те, що подібні незаконні дії та бездіяльність поліцейських можна оскаржити лише під час підготовчого провадження в суді (див. статтю 303 КПК України), тобто через невизначений проміжок часу, який не залежить від особи і може бути доволі тривалим, а також через те, що в межах кримінального провадження суд не може захистити порушене право на приватність (захист персональних даних), оскільки вирішує інші питання.

Тому така судова практика також ставить під сумнів наявність в Україні ефективного механізму захисту права особи на приватність, в тому числі, на захист її персональних даних.

3. Потенційні загрози для свободи слова та права на приватність в Інтернеті в Україні:

- 1) Загроза витоку персональних даних (прізвища та імені, номеру телефону, електронної пошти, реквізитів банківської картки, включаючи CVV2) та втрати грошових коштів у зв'язку із поширенням у соціальній мережі “Фейсбук” фейкової

¹⁶https://humanrights.org.ua/material/roskomnagljad_domigsjia_vid_nimeckogo_provajdera_blokuvannija_sajtu_vidannija_ukrajinskij_tizhden

¹⁷ <http://www.reyestr.court.gov.ua/Review/82822611>

¹⁸ <http://www.reyestr.court.gov.ua/Review/82946619>

реклами ПриватБанку, яка пропонує пройти опитування, під час якого збирає зазначену інформацію¹⁹.

- 2) Ризик втрати доступу до особистих акаунтів в соцмережах та втрати реквізитів банківських карток внаслідок шахрайської схеми, яка передбачає, що у месенджерах поширюється новина про те, що компанія Adidas нібито проводить акцію і безкоштовно роздає взуття і щоб отримати подарунок,- пропонується перейти за посиланням у повідомленні. Однак, за вказаним URL – знаходиться сайт, який здатний вкрасти особисту інформацію й паролі²⁰.
- 3) YouTube вимагає від UATV під загрозою блокування видалити відео-інтерв'ю керівника інформаційного офісу “Хізб ут-Тахрір” в Україні Фазилом Амзаєвим, яке було опубліковано в 2017 році. В ньому повідомляється про обшуки кримчан. Підставою таких вимог є повідомленням Роскомнадзору про те, що зазначені матеріали порушують Федеральний закон РФ №149-ФЗ “Про інформацію, інформаційні технології і про захисту інформації”²¹.
- 4) Російські хакери створюють фейкові додатки популярних програм для Android, зокрема Skype, Signal і PornHub з метою шпигування. У фейкові версії вбудовують шкідливе розширення Monocle, що може зчитувати зображення з екрана смартфона в будь-який час, і передавати його в Росію²².
- 5) Доступність в інтернеті додатку DeepNude, який за допомогою штучного інтелекту «роздягає» людей на фото, що може завдати шкоди життю людей²³.

Загалом в результаті моніторингу у липні 2019 виявлено **34 порушення цифрових прав**, а саме: **9** порушень цифрових прав **загального характеру**, з яких **3** стосуються доступу до Інтернету, **6** - порушення права вільно обирати членів парламенту (порушення стосувались, зокрема, законодавчих обмежень щодо ведення передвиборної агітації, правил інформування та проведення передвиборної агітації під час виборів тощо). Крім того, виявлено **25** порушень цифрових прав **індивідуального характеру**, з яких **23** випадків стосується порушень права на свободу вираження поглядів, а **2** - права на приватне життя та захист даних.

Крім того, виявлено **5** загроз для для свободи слова та права на приватність в Інтернеті в Україні.

¹⁹<https://v-variant.com.ua/tema/83593-po-seti-guljaet-rossijskij-privatbank-kotoryj-voruet-u-klientov-nastojaschego-banka-dengi-kak-ego-raspoznat-i-hto-delat-foto.html>

²⁰<https://www.obozrevatel.com/ukr/economics/fea/adidas-darue-tisyachi-par-vzuttya-ukrainsi-stayut-zhertvami-masshtabnoi-shemi.htm>

²¹<https://uatv.ua/cherez-povidomlennya-roskomnadzoru-youtube-vymagaye-vid-uatv-vydalyty-video-pro-obshuky-krymchan/>

²²<https://ukrainian.voanews.com/a/monocle-app/5016847.html?fbclid=IwAR3YgMctJ5vJK0v6LH3pUyzvAKhKR6p6J2cZs7Y0Tzn3R4yNiaFioRPNn6Q>

²³https://ms.detector.media/web/cybersecurity/kopii_dodatku_scho_rozdyagae_lyudey_na_foto_vilno_dos_tupni_u_merezhi_the_verge/