УДК 340 : 004
DOI https://doi.org/10.32782/2524-0374/2022-11/105

ПОЛІТИКО-ПРАВОВІ ПРОБЛЕМИ ВПЛИВУ СОЦІАЛЬНИХ МЕРЕЖ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ДЕРЖАВИ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

POLITICAL AND LEGAL PROBLEMS OF THE INFLUENCE OF SOCIAL NETWORKS ON THE INFORMATION SECURITY OF THE STATE IN THE CONDITIONS OF MARTIAL LAW

Ковальчук Л.В., студентка IV курсу юридичного факультету
Донецький національний університет імені Василя Стуса

Міхайліна Т.В., д.ю.н., професор,
професор кафедри теорії, історії держави і права та філософії права
Донецький національний університет імені Василя Стуса

Метою наукової статті є з'ясування основних політико-правових проблем впливу соціальних мереж на інформаційну безпеку держави в умовах військового стану, а також внесення пропозицій та рекомендацій щодо зниження відповідних ризиків.

Проаналізовано динаміку розвитку соціальних мереж в Україні за останні роки, структуру користувачів різних соціальних мереж, а також позитивні моменти і ризики їхнього глибокого проникнення у соціум під час військових дій.

Виявлено, що на сучасному етапі держава визначає одним із пріоритетних напрямків забезпечення інформаційної безпеки в соціальних мережах, однак конкретного механізму дій для протидії випадкам злочинного впливу у соцмережах досі не напрацьовано. Також понятєвий апарат у досліджуваній сфері має суттєві недосконалості. Зокрема, законодавство України не містить легального визначення таких понять як «соціальна мережа», «акант», що потребує доопрацювання.

Зроблено висновок, що серед першочергових заходів боротьби з інформаційними загрозами в соціальних мережах слід виділити систематизацію законодавчої бази, шляхом прийняття окремого закону про соціальні мережі, що повинен містити основні поняття, перелік дій, що будуть вважатися неправомірними, та методи боротьби з ними.

Наголошується, що варто забезпечити координацію органів кіберполіції задля виявлення фактів оприлюднення забороненого контенту. Особливої уваги у даному аспекті заслуговує створення такої програми, де будь-який свідомий громадянин може надіслати інформацію про наявність неправомірно оприлюдненої інформації з посиланням на відповідний акаунт. Вважаємо, що така практика сприятиме більш ефективному виявленню правопорушень в інформаційній сфері.

Крім того, акцентується увага на тому, що у сучасному digital-суспільстві інформаційна безпека держави тісно пов'язана з інформаційною культурою особи. Причому підвищення рівня інформаційної культури має забезпечуватися комплексом юридичних та неюридичних засобів. Було виявлено, що під час військової агресії інформаційна культура українців підвищилася експоненціально природнім шляхом. Це підтверджує чинник зберігання інформаційної тиші у ситуаціях, коли державні органи та посадові особи зверталися до населення із відповідним закликом.

Ключові слова: інформаційна безпека, інформаційна культура, інформаційне суспільство, держава, функції держави, функції права, соціальні мережі, юридична відповідальність, військовий стан.

The purpose of the scientific article is to clarify the main political and legal problems of the impact of social networks on the information security of the state under martial law, as well as to make suggestions and recommendations for reducing the corresponding risks.

The article analyzes the dynamics of the development of social networks in Ukraine in recent years, the structure of users of various social networks, as well as the positive aspects and risks of their deep penetration into society during military operations.

It is revealed that at the present stage, the state defines one of the priority areas for ensuring information security in social networks, but a specific mechanism of action to counteract cases of criminal influence in social networks has not yet been developed. Also, the conceptual framework in the field under study has significant imperfections. In particular, the legislation of Ukraine does not contain a legal definition of such concepts as "social network", "account", which requires revision.

It is concluded that among the priority measures to combat information threats in social networks, it is necessary to highlight the systematization of the legislative framework by adopting a separate law on social networks, which should contain basic concepts, a list of actions that will be considered illegal, and methods of combating them.

It is noted that it is necessary to ensure the coordination of cyber police bodies to identify the facts of publication of prohibited content. Special attention in this aspect deserves the creation of such a program, where any conscious citizen can send information about the presence of illegally published information with a link to the corresponding account. We believe that this practice will contribute to more effective detection of violations in the information sphere.

In addition, attention is focused on the fact that in a modern digital society, the information security of the state is closely linked to the information culture of an individual. Moreover, improving the level of information culture should be provided by a set of legal and non-legal means. It was found that during the military aggression, the information culture of Ukrainians increased exponentially in a natural way. This is confirmed by the factor of maintaining information silence in situations where state bodies and officials appealed to the population with a corresponding appeal.

Key words: information security, information culture, information society, state, state functions, law functions, social networks, legal responsibility, martial law.

Вступ. В умовах військової агресії з боку Російської Федерації актуальності набули питання, які ще донедавна вважалися малозначними. Так, військові дії ведуться не лише на всій території України, а й на інформаційному полі також. Блогінг, який ще донедавна вважався розважальною сферою, зараз набув ознак журналістської діяльності. Окремі інфлюенсери публікують велику кількість інформації, щоб донести її до широкого кола спостерігачів, що характеризується досить двояко. З однієї сторони, більшість блогерів усвідомлюють, що їхня аудиторія доволі різна і складається не лише з українських спостерігачів, а й з російських та білоруських, а отже є велика можливість донести реальну інформацію до деяких з них. А з іншої, публікуючи щось у соціальних мережах, люди не часто замислюються, яким чином та чи інша інформація може вплинути на хід воєнних подій.

Все частіше можна спостерігати, як фотографії переміщення збройних сил України, воєнної техніки і навіть місця вибуху стають причиною застосування окупаційної зброї, що й призводить до втрат та розрухи. Окрім того, масові потоки інформації, що розповсюджується у соцмережах, не лише зашкоджують психологічному здоров'ю населення, а й впливають на інформаційну безпеку держави загалом. Причому інформаційна безпека визнача-

ється важливим напрямом державної політики у сфері національної безпеки і оборони в положеннях Конституції України, Законах України: «Про національну безпеку України», «Про Концепцію Національної програми інформатизації», «Про оборону України», у Доктрині інформаційної безпеки України тощо.

Однак, соціальні мережі характеризуються як платформа для вільної комунікації, а отже, ймовірність отримання точних даних про особу, з якою спілкуєшся, є дуже низькою. А це, у свою чергу, зумовлює анонімність зловмисників та нерідко фактично відсутність реального притягнення таких осіб до відповідальності. З огляду на вказане постає необхідність в аналізі інформаційної безпеки держави у соціальних мережах в аспекті сучасної політико-фронтової ситуації.

Аналіз останніх наукових досліджень і публікацій. Правову оцінку вказаним проблемам надавав Д. Овчаров, аналізуючи останні новації у законодавстві України, що стосуються інформації та її впливу на безпеку держави [1], О. Марущак досліджував інформаційний фронт в українських медіа [2], однак питання інформаційної безпеки держави у соціальних мережах в умовах військового стану висвітлені досить обмежено, здебільшого у публіцистичних, а не наукових виданнях, що і зумовлює актуальність обраної теми дослідження.

Метою статті є з'ясування основних політико-правових проблем впливу соціальних мереж на інформаційну безпеку держави в умовах військового стану, а також внесення пропозицій та рекомендацій щодо зниження відповідних ризиків.

Виклад основного матеріалу. Стрімкий розвиток цифровізації та інформатизації пришвидшив процеси інтеграції світового масштабу. Сучасні способи комунікації охопили буквально увесь світ, а соціальні мережі стали чинником, що здійснює вплив на розвиток усього суспільства. Саме вони є одним з найзначущих джерел інформації, саме вони сприяють швидкому обміну даними і саме вони впливають на усі процеси, що відбуваються як всередині окремої держави, так і у світі загалом.

Зокрема, за статистикою відвідування соціальних мереж, наведеної компанією GlobalLogic, вказується, що на початку 2020 року в Україні було зареєстровано 19 мільйонів користувачів, у 2021 році цифра досягла 26 мільйонів. Водночас, проникнення соцмереж зросло наполовину: у них були зареєстровані 60 відсотків населення країни, тоді як у січні 2020 року було трохи більше ніж 40 відсотків [3]. А за останній рік, за даними тієї ж компанії, в Україні зросла кількість користувачів соцмереж – від 60% населення у 2021 році до 76,6% у липні 2022. Повномасштабне вторгнення призвело до того, що багато українців почали використовувати соцмережі як джерело інформації. Найпопулярнішим для цього виявився Telegram – його обирало 66% користувачів. Друге та третє місце за інформативністю зайняли YouTube (61%) та Facebook (58%). Тобто, на сьогодні серед Інтернет-користувачів важко знайти людину, яка не мала б профілю хоча б в одній соціальній мережі, і це не дивно, оскільки усі процеси комунікації здійснюються саме за допомогою новітніх додатків. Однак, поширення такого попиту на соціальні мережі сприяє не лише активній інформатизації суспільства, а й зумовлює зростання негативного впливу як на окремих осіб, так і на групу, населення та навіть державу [4].

Інформація стала знаряддям війни, і це знаряддя активно поширюється через соціальні мережі. Як зазначають Г. Фарел та Д. Дрезнер [5], відносною перевагою блогів у політичному дискурсі є низька вартість публікацій в режимі реального часу. Негайно відгукуючись на будь-які події – від президентських дебатів до терористичних атак – блогери мають змогу оприлюднити свої коментарі безпосередньо ще до того, як в інформаційному просторі з'являться перші відгуки інших форм засобів масової інформації. Дану ситуацію спостерігаємо і в умовах війни з Росією. Блогери стали ще однією вагомою зброєю, мета якої висвітити реальні події, показати правду. Однак, ця зброя може діяти як на користь державі, так і на шкоду. Зокрема, можна спостерігати, як Російська Федерація використовує армію лояльних до режиму блогерів (яких називає військовими кореспондентами) для просування у маси позиції, вигідної правлячій верхівці.

Крім того, у зв'язку з поширенням через соціальні мережі інформації про пересування техніки, українських військових тощо, ворог почав використовувати вказані дані на власну користь. Тому у відповідь на вказану проблему, Верховна Рада України запровадила кримінальну відповідальність за фото- та відеозйомку переміщень Збройних сил України в умовах воєнного або надзвичайного стану. А Кримінальний кодекс України, відповідно, було доповнено статтею 114-2: «Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану» [6]. Дана норма передбачає кримінальну відповідальність за розповсюдження матеріалів, що можуть бути використані ворогом.

Ж. Грушко зазначає, що означає термін «несанкціоноване поширення». Це поширення інформації до її офіційного оприлюднення Генштабом ЗСУ або без його письмового дозволу на швидше оприлюднення. Також вона вказує, що відповідальність настає і при вчиненні злочину з необережності. «Якщо поширення вищевказаної інформації відбулося умисно, з корисливих мотивів, з метою передачі її ворогові, за попередньою змовою групи осіб або ж таке поширення спричинило тяжкі наслідки (смерть людей/групи людей), то відповідальність посилюється – позбавлення волі на строк від 8 до 12 років. При цьому, спосіб поширення цієї інформації може бути будь-який. До прикладу, шляхом розміщення фото, відео, аудіозаписів у соцмережах, приватне листування через емейл чи телефонні дзвінки». Серед інформації, яку заборонено публікувати, зазначають: напрям руху ракет та місце влучення; назви вулиць, зупинок громадського транспорту, магазинів, ТРЦ, підприємств, заводів, фабрик тощо; переміщення українських військових та військових об'єктів; роботу ППО; адреси, візуальне розташування чи координати ведення боїв; місця обстрілів та потрапляння снарядів; номери транспортних засобів та бронетехніки; потерпілих, поранених чи загиблих осіб [7].

Проте варто зазначити певну недосконаліть законодавства України. Так, жоден нормативно-правовий акт не містить визначення таких термінів як «соціальна мережа» та «акаунт». Проте акаунт можна розглядати як веб-сторінку, термін якої зазначено в Законі України «Про авторське право та суміжні права». Відповідно до вказаного Закону, веб-сторінка – це складова веб-сайту, що може містити дані, електронну (цифрову) інформацію, інші об'єкти авторського та/або суміжних прав тощо [8]. З цього постає питання, хто повинен відповідати за розміщену інформацію на акаунті.

В Законі України «Про авторське право та суміжні права» вказується, що власник веб-сторінки – це особа, яка є володільцем облікового запису, що використовується для розміщення веб-сторінки на веб-сайті, та управляє і/або розміщує електронну (цифрову) інформацію в межах такої веб-сторінки. Тобто, власник веб-сайту і власник веб-сторінки не є тотожними поняттями, а отже, якщо власник веб-сторінки розміщує якусь інформацію, то відповідальність за її розміщення несе особисто він.

Однак, аналізуючи природу соціальних мереж, було встановлено, що більшість осіб, які публікують вказаного виду інформацію, користуються так званими «фейковими»

(неправдивими) сторінками, що ускладнює пошук даної особи. Підтверджує зазначену інформацію статистика GlobalLogic, де зазначається, що рівень проникнення серед 18-27-річних в найбільш популярній серед молоді соціальній мережі Instagram сягає більш ніж 100% [3]. І саме цей аспект зумовлює широке розповсюдження неправомірної інформації, оскільки більшість відчуває безкарність.

Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року, визначає, що «хоча право на приватність (захист конфіденційної інформації про особу, невтручання в особисте життя) є одним з основних прав людини, що закріплено в Загальній декларації прав людини, Конвенції про захист прав людини і основоположних свобод, інших міжнародних документах, а також конституціях більшості держав світу, цифрові трансформації змінюють і цю сферу. Збільшення кількості соціальних мереж, їх інтегрованість з іншими соціальними сервісами повсякденного користування, а також специфіка організації всесвітньої мережі Інтернет ставлять під загрозу гарантії права особи на приватність. Спроби врегулювати цю проблему тривають, формуються нові підходи у забезпеченні балансу права на приватність та інформаційної безпеки держави» [9].

Тобто, держава визначає одним із пріоритетних напрямків забезпечення інформаційної безпеки в соціальних мережах, однак з формулювання стає зрозумілим, що конкретного механізму дій для протидії випадкам злочинного впливу в соцмережах досі не існує, а отже пріоритетом для держави є забезпечення дієвої системи виявлення правопорушників та активна боротьба з ними, адже в сучасних умовах від дієвості кіберполіції залежить життя багатьох людей.

У той же час, акцентується увага на тому, що у сучасному digital-суспільстві інформаційна безпека держави тісно пов’язана з інформаційною культурою особи. Причому підвищення рівня інформаційної культури має забезпечуватися комплексом юридичних та неюридичних засобів. Було виявлено, що під час військової агресії інформаційна культура українців підвищилася експоненціально природнім шляхом. Це підтверджує чинник зберігання інформаційної тиші у ситуаціях, коли державні органи та посадові особи зверталися до населення із відповідним закликом.

Висновки. Таким чином, з огляду на вищенаведене варто зробити висновок, що серед першочергових заходів боротьби з інформаційними загрозами в соціальних мережах слід виділити систематизацію законодавчої бази, шляхом прийняття окремого закону про соціальні мережі, що повинен містити основні поняття, перелік дій, що будуть вважатися неправомірними, та методи боротьби з ними.

Наголошується, що варто забезпечити координацію органів кіберполіції задля виявлення фактів оприлюднення забороненого контенту. Особливої уваги у даному аспекті заслуговує створення такої програми, де будь-який свідомий громадянин може надіслати інформацію про наявність неправомірно оприлюдненої інформації з посиланням на відповідний акаунт. Вважаємо, що така практика сприятиме більш ефективному виявленню правопорушень в інформаційній сфері.

Крім того, акцентується увага на тому, що у сучасному digital-суспільстві інформаційна безпека держави тісно пов’язана з інформаційною культурою особи. Причому підвищення рівня інформаційної культури має забезпечуватися комплексом юридичних та неюридичних засобів. Було виявлено, що під час військової агресії інформаційна культура українців підвищилася експоненціально природнім шляхом. Це підтверджує чинник зберігання інформаційної тиші у ситуаціях, коли державні органи та посадові особи зверталися до населення із відповідним закликом.

ЛІТЕРАТУРА

1. Кримінальна відповідальність під час воєнного стану: законодавчі новели. *Асоціація правників України*. 2022. URL: https://uba.ua/ukr/news/9115/ (дата звернення: 27.03.2022).
2. Марущак О. Голова Держспецзв’язку Юрій Щиголь: «Медіа України – серед основних цілей ворога» – інтерв'ю. *Сьогодні*. 2022. URL: www.segodnya.ua/ua/strana/podrobnosti/golova-derzhspeczv-yazku-yuriy-shchigol-media-ukrajini-sered-osnovnih-ciley-voroga-interv-yu-1612338.html (дата звернення: 27.03.2022).
3. Facebook та Instagram в Україні. *Plusone social impact*. 2021. URL: https://plusone.com.ua/research/Facebook%20%D1%82%D0%B0%20Instagram%20%D0%B2%20%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96%20-%202021%20%D0%BB%D0%B8%D0%BF%D0%B5%D0%BD%D1%8C.pdf (дата звернення: 28.03.2022).
4. Найпопулярніші соцмережі в Україні під час війни – дослідження Global Logic. *https://mezha.media*. 2022. URL: https://mezha.media/2022/08/06/naypopuliarnishi-sotsmerezhi-v-ukraini-pid-chas-viyny-doslidzhennia-global-logic/ (дата звернення: 26.11.2022).
5. Farell H., Drezner D.W. The power and politics of blogs. *Springer Science+Business Media*. 2007. Sept. 12. URL: www.danieldrezner.com/research/blogpaperfinal.pdf (дата звернення: 01.04.2022).
6. В Україні запровадили кримінальну відповідальність за публікацію інформації про пересування ЗСУ. *1plus1*. URL: https://1plus1.ua/novyny/v-ukraini-zaprovadili-kriminalnu-vidpovidalnist-za-publikaciu-informacii-pro-peresuvanna-zsu (дата звернення: 29.03.2022).
7. За які фото і відео в соцмережі можна потрапити до тюрми? Пояснює вінницька адвокатка. *20minut.ua*. URL: https://vn.20minut.ua/Podii/za-yaki-foto-i-video-v-sotsmerezhi-mozhna-potrapiti-do-tyurmi-poyasnyu-11548448.html (дата звернення: 29.03.2022).
8. Про авторське право і суміжні права: Закон України від 23 грудня 1993 р., № 3792-XII. *Відомості Верховної Ради України*. 1994. № 13. Ст.64.
9. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021р., № 685/2021. URL: https://zakon.rada.gov.ua/laws/card/685/2021 (дата звернення: 02.04.2022).