УДК 004.73/-057.36

МІЖНАРОДНО-ПРАВОВИЙ ДОСВІД ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ ВІЙСЬКОВОСЛУЖБОВЦЯМИ ЗБРОЙНИХ СИЛ ТА СПІВРОБІТНИКАМИ ПРАВООХОРОННИХ ОРГАНІВ

INTERNATIONAL LEGAL EXPERIENCE USING SOCIAL NETWORKS PERSONNEL OF THE LAW ENFORCEMENT

Черниш Р.Ф.,
кандидат юридичних наук, доцент кафедри правознавства Житомирського національного агроекологічного університету

У статті досліджено міжнародно-правовий досвід у сфері регламентації використання мережі Інтернет та соціальних спільнот військовослужбовцями. На його підставі, зважаючи на необхідність недопущення витоку інформації про сили та засоби, а також специфіку задач, які виконуються в районі проведення АТО, запропоновано першочергові зусилля у вказаній сфері спрямувати на розробку відповідних інструкцій, в яких необхідно передбачити основні засади поведінки, специфіку налаштування безпеки особистої сторінки або блогу в соціальних інтернет-сервісах, заборони, яких необхідно дотримуватися, використовуючи інтернет, а також відповідальність за порушення останніх.

Ключові слова: соціальні мережі, віртуальна спільнота, інтернет, військовослужбовці, співробітники правоохоронних органів, антитерористична операція, район проведення антитерористичної операції.

В статье исследован международно-правовой опыт в сфере регламентации использования сети Интернет и социальных сообществ военнослужащими. На его основании, учитывая необходимость не допустить утечку информации о силах и средствах, а также специфике задач, которые выполняются в районе проведения АТО, предложено первоочередные усилия в указанной сфере направить на разработку соответствующих инструкций, в которых необходимо предусмотреть основные принципы поведения, специфику настройки безопасности личной страницы или блога в социальных интернет-сервисах, запреты, которые необходимо соблюдать, используя интернет, а также ответственность за нарушение последних.

Ключевые слова: социальные сети, виртуальное сообщество, інтернет, военнослужащие, сотрудники правоохранительных органов, антитеррористическая операция, район проведения антитеррористической операции.

In the article investigated the international legal experience in the regulation of the use of the Internet and social network communities soldiers. On its basis, given the need to prevent leaks of troops and equipment, and the specific tasks performed in the area of anti-terrorist operation proposed priority efforts in this sphere directed to the development of appropriate guidelines which should provide basic principles of conduct, specific security settings personal page or blog in social Internet services, prohibitions, to be followed using the Internet network, as well as responsibility for violation of the latter.

Key words: social networks, virtual communities, online, military, law enforcement, anti-terrorist operation, area of anti-terrorist operations.

Постановка проблеми. Зважаючи на стан розвитку інформаційно-комунікаційних технологій, дедалі більшу увагу науковці приділяють вивченню зростання ваги інтернету та соціальних мереж у всіх аспектах суспільного життя. Не є виключенням й військова сфера.

Особливої актуальності вищевказане набуло у зв'язку з реалізацією протягом останніх років спеціальними службами Російської Федерації (РФ) нових форм та методів ведення «гібридної війни» – інформаційного впливу на свідомість громадян, протиправного використання даних, здобутих із відритих джерел, у першу чергу щодо військовослужбовців ЗС України (інших правоохоронних органів) тощо. Зазначене, окрім можливого несанкціонованого доступу до відомостей, що становлять державну чи службову таємницю (дислокація підрозділів, кількісний чи якісний склад, наявність на озброєнні військових засобів ураження тощо), як свідчать реалії сьогодення, призводить, на жаль, і до більш негативних наслідків – загибелі особового складу на сході України.

Метою статті є аналіз міжнародного досвіду у сфері використання військовослужбовцями Збройних сил та співробітниками правоохоронних органів інтернету і соціальних спільнот заради вироблення конструктивних пропозицій щодо механізму, змісту та об'єму поширення представниками силового блоку, що беруть участь в антитерористичній операції на сході України (АТО) допустимої інформації .

Виклад основного матеріалу. Усвідомлення в умовах сьогодення ролі інтернету та соціальних мереж (формування громадської думки, каталізатор протестного потенціалу, поширення тенденційної інформації тощо) змушує передові держави світу інвестувати значні кошти в розвиток та забезпечення безпеки інтернету. Процес боротьби в інформаційному просторі за «думки людей» створив передумови до визнання соціальних мереж як інструменту інформаційного протиборства. Таким чином, соціальні мережі стали ареною сучасних інформаційних війн і засобом висвітлення різних військових та політичних процесів протиборчих сторін.

Протягом останнього часу відповідні інтернет-ресурси та офіційні тематичні спільноти в соціальних мережах (Facebook, ВКонтакте, Twitter і т.д.) активно використовують й представники силових відомств нашої держави. Щоденно на інформаційних ресурсах Міністерства оборони, Служби безпеки, Міністерства внутрішніх справ України тощо оприлюднюється відкрита інформація, яка стосується всіх аспектів діяльності військовослужбовців та співробітників зазначених структур. Водночас, якщо дані, які публікуються на офіційних інтернет-ресурсах, проходять жорстку цензуру на предмет можливості витоку інформації з обмеженим доступом, у разі використання соціальних мереж у приватних цілях відомості поширюються конкретним суб'єктом на власний розсу майже без обмежень.

Для представників силового блоку інтернет став неоднозначним явищем: з одного боку, його використання створює значний потенціал щодо налагодження процесу комунікації (особливо з молоддю), а з іншого − є джерелом потенційного витоку інформації, яка має стратегічне значення для національної безпеки і, за певних умов, може бути використана «спецслужбами» т. зв. «ДНР»/«ЛНР» чи країни-агресора проти України.

Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування військової сили, послабити або завдати значної шкоди безпеці державі−протагоністу, яка не має дієвої системи захисту від негативних інформаційних впливів [9].

У ЗМІ та мережі Інтернет неодноразово фіксувались випадки поширення відомостей щодо дислокації, розгортання та переміщення підрозділів Збройних сил України та інших правоохоронних органів, стану бойової та мобілізаційної готовності, технічного стану військових засобів ураження, військової та спеціальної техніки, рівня матеріального забезпечення та морально-психологічного стану військовослужбовців та співробітників правоохоронних органів, специфіки виконання робіт підприємствами оборонно-промислового комплексу із розробки, виготовлення, ремонту, модернізації озброєнь та військової техніки й іншої інформації, яка ставить під загрозу успішне проведення антитерористичної операції на сході України. Також доволі часто військовослужбовці розміщують у соціальних мережах особисті фото з району проведення АТО, зроблені на фоні місцевості, в якій дислокується підрозділ. Однак до уваги не береться той факт, що наявне програмне забезпечення дозволяє ідентифікувати місцевість та визначити конкретні координати місця дислокації.

Водночас, ймовірно, мало хто задумується про те, що соціальні мережі є ідеальним інструментом для стеження за користувачами. Їх інтернет-активність за допомогою сучасного програмного забезпечення автоматично аналізується, на основі чого можна отримати відповідні матеріали з посиланнями на інформацію про особу: особисті дані, місцезнаходження, пересування, уподобання, коментарі, репости тощо.

Отримана інформація використовується, зокрема, й з метою психологічного тиску на особовий склад. Так, ще в 1994–1996 рр., під час операції ЗС США на Гаїті під умовною назвою «Підтримка демократії» на номери військовослужбовців національної армії здійснювалися дзвінки, розсилалися смс-повідомлення із закликами не чинити опору.

Під час операції «Свобода Іраку» американці провели широкомасштабну акцію за допомогою електронної пошти. Зокрема, розсилалися послання арабською мовою іракським генералам із закликами до невиконання наказів С. Хусейна. У цих листах з позначкою «важлива інформація» були відсутні відкриті загрози, проте їх підтекст був зрозумілий. Вони містили рекомендації надавати інспекторам ООН відомості про місцезнаходження зброї масового ураження. В електронних повідомленнях, складених провідними американськими військовими психологами, підкреслювалося, що, якщо громадяни Іраку допоможуть запобігти використанню зброї масового ураження, то Сполучені Штати зроблять все необхідне, щоб захистити їх самих і членів їх сімей. Водночас увагу адресатів звертали на те, що відмова від співпраці спричинить «серйозні наслідки», а ті, хто «допоможе застосувати хімічну, біологічну чи ядерну зброю, будуть вважатися військовими злочинцями» [6].

Вже понад два роки прихильники т. зв.«ДНР»/«ЛНР» активно використовують інформаційний простір із метою впливу на свідомість громадян, що проживають на тимчасово підконтрольній бойовикам території України, як у власному «медійному ресурсі», так і в засобах масової інформації Російської Федерації [10]. Однак об'єктом вищевказаної протиправної діяльності стали й представники силового блоку, які виконують завдання в районі проведення АТО, та їх рідні. Зокрема, відповідно до наявної в Міністерстві оборони України інформації, фахівці російських інформаційно-психологічних операцій намагаються посіяти паніку в колі захисників Вітчизни шляхом розсилання українським військовим на передовій провокативних смс-повідомлень, де ідеться про те, що нібито варто покидати свої позиції, бо всіх «зрадили і здали» тощо [8].

Яскравим прикладом негативних наслідків несанкціонованого поширення інформації військовослужбовцем в соціальній мережі є скасування у 2010 р. ізраїльською армією військової операції через пост у Facebook солдата, який написав: «У середу зачищаємо Катану та в четвер, якщо на те воля Божа, повертаємося додому». Виданий іншими військовими, він постав перед трибуналом і був покараний. Однак це далеко не єдиний випадок мимовільного злиття стратегічної інформації в лавах ізраїльської армії. Після цих подій в ізраїльських Збройних силах було створено спеціальний підрозділ з метою моніторингу витоку стратегічної інформації та проведено кампанію з роз'яснення, якого роду відомості не варто розміщувати в соціальних мережах [7], а за кожним ЗМІ було закріплено військового цензора. Правила цензурування дуже жорсткі: жодних показів техніки, дуже жорстка заборона на повідомлення про кількість жертв серед військових. Журналістам не дозволяють знімати навіть характер ушкоджень, завданих інфраструктурі внаслідок артилерійських обстрілів, із метою недопущення оцінки ворогом точності влучання й коригування координат.

На сайті Державного департаменту оборони США було розміщено оголошення, в якому зазначалося, що американським військовослужбовцям офіційно дозволено користуватися соціальними мережами, але з пристроїв, не під'єднаних до інформаційної системи армії. Цей дозвіл отримали навіть військовослужбовці, що перебували на полі бою. До того часу питання використання соціальних мереж не регламентувалося в офіційних документах. Департамент оборони США уточнює, що командування різних військових частин має перервати будь-який зв'язок за певних обставин [2]. Загалом, в американській армії за роботу з медіа відповідає прес-офіцер, але й командир підрозділу зобов'язаний надавати інформацію журналістам. Солдатам також дозволено спілкуватись із медійниками. Однак, якщо запитання не в їхній компетенції, вони це пояснюють. Американських військовослужбовців вчать роботі з медіа, і цей досвід не зайвий для українців. Зокрема, підполковник Кайл Рід, командир 173-ї аеромобільної бригади США з цього приводу зазначив: «Кожній місії, яку ми виконуємо, передує відповідна підготовка у сфері зв'язків із громадськістю, і це включає не лише співпрацю з медіа, але і те, яку інформацію можна викладати в соціальних мережах. Ми їм не забороняємо це робити, але просимо добре подумати, що вони викладають і що хочуть донести до тих, хто це читатиме» [4].

Основним нормативним документом, який регламентує процедуру використання військовослужбовцями США соціальних спільнот, є «Керівництво по соціальним медіа ЗС США» ("U.S. Army Social Media Handbook") [3].

Головна ідея документу – визначення правил користування соціальними інтернет-сервісами для військовослужбовців ЗС США та членів їх сімей. У ньому наводяться приклади оформлення сторінок і блогів та зазначаються певні заборони під час роботи у соціальних інтернет-сервісах. Це, зокрема, заборона на розміщення інформації щодо дислокації та заходів, що плануються, фотографій військових об'єктів та техніки, приватної інформації про товаришів по службі та своїх близьких, заборона на додавання у друзі своїх начальників із метою додержання субординації тощо.

Міністерством оборони Франції з метою протидії небезпеці, яка пов'язана зі спілкуванням у соціальних мережах, у 2012 р. розроблено відповідну інструкцію поведінки для військовослужбовців [4], мета якої допомогти у використанні соціальних мереж. Зазначений нормативний акт містить кілька розділів, кожний з яких доповнено практичними порадами: повага до секретності операцій, комунікація приватної особи, комунікація в професійному середовищі. Також наведено конкретні приклади, коли військовослужбовці некоректно використовували свою присутність у соціальних медіа. До найбільш поширених ризиків належать недостатня перевірка параметрів конфіденційності, геолокалізація своєї позиції під час військових операції, розміщення фото та відео, які містять стратегічну інформацію.

У Великобританії також розроблено та впроваджено кодекси поведінки в соціальних мережах для державних службовців та військовослужбовців, зокрема, в «Соціальному керівництві користування засобами масової інформації для державних службовців» (“Guidance. Social media guidance for civil servants: October 2014”). Головна ідея документу – визначення правил користування соціальними інтернет-сервісами для державних службовців загалом та військовослужбовців зокрема. Основні заборони націлені на нерозповсюдження інформації, яка не має «здорового глузду»; порушення Кодексу цивільної служби як під час службового, так і неслужбового користування; поширення інформації, щодо якої в державного службовця є сумніви; розповсюдження недостовірної та неперевіреної інформації тощо. У «Керівництві для військовослужбовців з використання соціальних медіа» (“Guidance For Service Personnel On The Use Of Social Media”) закріплено основні правила використання соціальних мереж вказаною категорією осіб.

Водночас основні заборони стосуються розповсюдження конфіденційної інформації, оскарження рішень керівництва Збройних сил та командування, можливості використання геотегів, коментування подій у хворобливому стані та стані сп’яніння, порушення авторських прав тощо [1].

В Ірландії функціонує інформаційний довідник (“Information Handbook”) для військовослужбовців, в якому закріплено правила поширення інформації в медіапросторі. Зокрема, регламентуються основи службового та приватного використання соціальних інтернет-сервісів; визначено порядок акредитації інтернет-ресурсів, які представляють ЗС у мережі; заборонено поширення інформації без попереднього дозволу компетентних органів; заборонено поширення інформації, яка дискредитує ЗС; заборонено поширення контенту політичного забарвлення тощо [1].

Що ж до таких країн, як Китай та Індія, там військовослужбовцям заборонено реєстрацію в соціальних мережах, а також коментування в мережі Інтернет будь-якої інформації.

Висновки. Проаналізувавши досвід Збройних сил провідних країн світу у сфері регламентації процедури використання військовослужбовцями та співробітників силового блоку соціальних мереж, можна дійти висновку, що вказана діяльність частково контролюється державою. З цією метою розроблено та імплементовано до законодавства ряд відомчих нормативно-правових актів.

На нашу думку, в Україні, незважаючи на здійснення вищим керівництвом держави ряду позитивних кроків у сфері забезпечення кібербезпеки (введення в дію Указами Президента України: від 13.02.2017 р. № 32/2017 Рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» та від 25.02.2017 р. № 47/2017 Рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Доктрину інформаційної безпеки України» тощо), заходи із нормативної регламентації використання інтернету та соціальних спільнот (насамперед, військовослужбовцями та співробітниками інших силових підрозділів, особовий склад яких виконує (виконував) завдання в районі проведення АТО, та членами їх сімей) є недостатніми.

Враховуючи вищевикладене, першочергові зусилля мають бути спрямовані на розробку на рівні Міністерства інформаційної політики України (з подальшим погодженнями з керівництвом силових підрозділів та відомчим впровадженням) відповідних інструкцій, в яких необхідно передбачити основні засади поведінки, специфіку налаштування інформаційної безпеки особистої сторінки або блогу в соціальних інтернет-сервісах, заборони, яких необхідно дотримуватися, використовуючи Інтернет-мережу, а також відповідальність за порушення останніх.

Що ж до заборон для військовослужбовців ЗС України та працівників або співробітників правоохоронних органів, на наш погляд, вони мають полягати:

– в обмеженні поширення в публічному доступі повних персональних даних (П.І.Б., адреса проживання, фото, номер мобільного телефону тощо);

– в обмеженні розповсюдження інформації (установчі дані, посилання, фото тощо) своїх близьких;

– заборона використання соціальних спільнот в інтернеті, почтових сервісів тощо, доступ до яких за спрощеною процедурою мають представники спеціальних служб країни-агресора («ВКонтакте», «Одноклассники», «Mail.ru» тощо);

– у забороні на розміщення службової інформації (розгортання та передислокація підрозділів (окремих військовослужбовців) ЗС України та правоохоронних органів (окремих працівників або співробітників правоохоронних органів): стан бойової та мобілізаційної готовності; технічний стан військових засобів ураження, військової та спеціальної техніки; рівень матеріального забезпечення та морально-психологічний стан військовослужбовців та співробітників правоохоронних органів; специфіка виконання робіт підприємствами оборонно-промислового комплексу із розробки, виготовлення, ремонту та модернізації озброєнь та військової техніки тощо);

– заборона розміщення фото військових обєктів та техніки;

– заборона поширення персональної інформації про інших військовослужбовців;

– заборона обговорення наказів командирів;

– заборона на використання геотегів тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Правила користування соціальними мережами військовослужбовцями за досвідом провідних країн світу [Електронний ресурс]. – Режим доступу : http://stratcom.co.ua/pravila-koristuvannya-sotsialnimi-merezhami-vijskovosluzhbovtsyami-za-dosvidom-providnih-krayin-svitu/.

2. [Електронний ресурс]. –Режим доступу : http://www.defense.gov/news/newsarticle.aspx?id=58117.

3. US Army Social Media Handbook [Електронний ресурс]. – Режим доступу : http://www.nationalguard.mil/Portals/31/Resources/SocialMedia/US%20Army%20Social%20Media%20Handbook%20(Jan.%202013).pdf

4. Американські інструктори попереджають: «Соціальні мережі – ідеальний інструмент для стеження за користувачами» [Електронний ресурс]. – Режим доступу : http://www.milnavigator.com/uk/amerikanskie-instruktora-preduprezhdayutsocialnye-seti-idealnyj-instrument-dlya-slezhki-za-polzovatelyami/.

5. Армія та соціальні мережі [Електронний ресурс]. – Режим доступу : http://wartime.org.ua/1758-armya-ta-socaln-merezh.html.

6. Завада А.А. Правила користування соціальними мережами військовослужбовцями за досвідом провідних країн світу [Електронний ресурс]. – Режим доступу : http://wartime.org.ua/960-nternet-nformacyna-vyna-zbroyn-konflkti.html.

7. Нові медіа: ризики та можливості для Збройних сил Французької Республіки [Електронний ресурс]. – Режим доступу : http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/novi-media-riziki-ta-mozhlivosti-dlja-zbroinikh-sil-fran/.

8. Сепаратисти шлють українським військовим провокативні СМСки [Електронний ресурс]. – Режим доступу : http://www.volynpost.com/news/46446-separatysty-shlyut-ukrainskym-vijskovym-provokatyvni-smsky-foto.

9. Черниш Р.Ф. Щодо окремих аспектів протидії інформаційному тероризму в сучасних умовах / Р.Ф. Черниш, І.М. Осауленко // Протидія терористичній діяльності: міжнародний досвід і його актуальність для України : матер. міжнар. наук.-практ. конф. (30 вересня 2016 р.). – Київ : Національна академія прокуратури України, 2016.

10. Черниш Р.Ф. Окремі кроки протидії сепаратизму в інформаційній сфері, як передумова реалізації євроінтеграційних процесів / Р.Ф. Черниш // [Електронний ресурс]. – Режим доступу : http://ir.znau.edu.ua/bitstream/123456789/5680/1/OKPSvISPREP_2016_427-430.pdf.