УДК 342: 341.4:343.974:343.346.8

Сивухін Владислав Сергійович – провідний науковий співробітник Національної академії внутрішніх справ, кандидат юридичних наук

Конституційні засади транскордонного доступу як форми міжнародного співробітництва у боротьбі з організованою кіберзлочинністю

У статті розглянуто проблеми застосування транскордонного доступу до комп'ютерних даних як форми взаємної правової допомоги з протидії організованій кіберзлочинності.

Ключові слова: *кіберзлочин, кіберпростір, організована кіберзлочинність, транскордонний доступ до комп'ютерних даних.*

Постановка проблеми. Технічне удосконалення телекомунікаційних систем глобального зв'язку і спрощення доступу до використання комп'ютерних технологій для широкого кола користувачів через персональні комп'ютери та мобільні пристрої, веде до трансформації злочинності, яка для реалізації протиправних намірів переміщується у кіберпростір. З цією метою як організовані злочинні угруповання наймають ІТ-фахівців (Хамаз, Аль-Каїда тощо), так і самі ІТ-фахівці створюють структуровані злочинні спільноти за мафіозними типами (наприклад, CarderPlanet) [1]. Члени таких угруповань, використовуючи відкритість Інтернет простору, обирають для вчинення злочинів території з вигідною для них юрисдикцією, залишаючись при цьому анонімними (використання сервісів анонімізації), що й зумовлює високий рівень латентності та низький рівень розкриття таких злочинів. Це актуалізує питання криміналістичного, правового характеру, зокрема, проблеми традиційного застосування юридичної відповідальності, поняття юрисдикції (дії нормативно-правового акту в кіберпросторі) та застосування процедурних положень міжнародних конвенцій з протидії кіберзлочинності.

Аналіз останніх досліджень і публікацій. Окремі питання протидії організованій злочинності у глобальному інформаційному середовищі розглядалися у працях вітчизняних і зарубіжних науковців: Д. С. Азарова,

П. Д. Біленчука, В. М. Брижка, В. М. Бутузова, О. Г. Волеводза, В. М. Волженкіної, В. Д. Гавловського, М. В. Гуцалюка, Р. А. Калюжного, М. В. Карчевського, В. В. Милинчука, С. С. Овчинського, В. П. Сабадаш, Т. Б. Сєітова, В. С. Цимбалюка, Л. Шеллі, В. П. Шеломенцева, Ф. Уільямса та інших.

Останнім часом в Україні з'явилось чимало публікацій з вказаної проблеми: А. В. Войцехівського, Є. В. Зозулі, А. І. Європіної, С. Г. Каланчі, О. М. Кравченка, О. В. Манжай, Н. І. Пашковського, М. І. Смирнова, Ю. В. Степанова, О. В. Шамари та інших. Праці зазначених науковців зробили істотний внесок у досліджувану проблему і дозволили автору використовувати низку важливих базових положень з проблем протидії організованій кіберзлочинності. Разом з тим, незважаючи на фундаментальне опрацювання окремих проблем міжнародної співпраці у боротьбі з організованою кіберзлочинністю і безумовну затребуваність праць названих учених і практиків, деякі проблемні питання міжнародного співробітництва залишилися охопленими не в повній мірі.

Так, на сьогодні в Україні відсутні комплексні дослідження, присвячені теоретичній та практичній проблемам застосування у правоохоронній діяльності транскордонного доступу до комп'ютерних даних, його відповідності конституційним положенням і доцільності його безпосередньої імплементації до вітчизняного законодавства, що обумовлює актуальність розгляду вказаного питання. У зв'язку з цим, здійснено спробу розв'язати теоретичні й практичні проблеми застосування транскордонного доступу до комп'ютерних даних.

Виходячи із зазначеного, **метою статті** є дослідження проблем застосування транскордонного доступу до комп'ютерних даних як форми міжнародного співробітництва з протидії організованій кіберзлочинності.

Досягнення поставленої мети реалізовувались через постановку та послідовне вирішення таких основних завдань: 1) дослідити особливості протиправного використання комп'ютерних технологій організованою злочинністю в телекомунікаційному просторі; 2) окреслити теоретичні, міжнародні та конституційно-правові проблеми застосування кримінальної юрисдикції у кіберпросторі; 3) обгрунтувати пропозиції щодо вироблення єдиного підходу до застосування транскордонного доступу як форми міжнародного співробітництва з протидії організованій кіберзлочинності.

Виклад основного матеріалу дослідження. Характерними рисами використання комп'ютерних технологій в телекомунікаційному просторі є їх універсальність, радикальність застосування, доступність та екстериторіальність, що у випадку їх протиправного застосування значно підвищує їх суспільну небезпечність. Як відмічає Сьюзанн В. Бреннер, "кіберзлочин" не вимагає фізичного зближення жертви та суб'єкта злочину в момент його вчинення, не підвладний обмеженням,

які існують у реальному, фізичному світі, що сприяє моментальному і багаторазовому (до декількох тисяч) вчиненню злочину. Це потребує швидкої реакції у відповідь [2].

Завдяки таким особливостям більшість "традиційних" злочинів, на яких спеціалізуються міжнародні організовані угруповання, із реального простору перейшли до віртуального (відмивання грошей, шахрайство з фінансовими ресурсами, торгівля наркотиками, зброєю, людьми, тероризм тощо). Тому, невипадково, ще у 1992 р. ООН віднесла злочини у сфері комп'ютерних технологій до переліку 14 видів транснаціональних організованих злочинів [3]. Одним із прогресивних кроків у виробленні єдиних підходів до протидії комп'ютерним злочинам стало прийняття в рамках Ради Європи Конвенції по боротьбі з кіберзлочинністю (23 листопада 2001 р.). У той же час, окремі положення Конвенції викликали критику під час Щорічної зустрічі експертів поліції "Боротьба з загрозою кіберзлочинності" (19–21 вересня 2012 р., Австрія), зокрема п. b. ст. 32 Конвенції [4].

Вказана норма регулює питання транскордонного доступу до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними. Іншими словами, чи можуть компетентні органи однієї держави одержати прямий доступ до бази даних, що знаходиться в сфері юрисдикції іншої держави, без залучення до цього (або повідомлення чи згоди) останнього. З цього приводу єдності у світового співтовариства немає [5]. Адже, далеко не всі країни (з-поміж тих, що входять до Ради Європи) ратифікували цей документ (зокрема, принципову позицію з цього питання посіла Російська Федерація).

З першого погляду, проведення дослідчих перевірок в українському сегменті кіберпростору не викликає правових питань. У той же час , як відмічає Аллан Р. Стейн, найбільш проблемною характеристикою мережі Інтернет з точки зору юрисдикційної політики є те, що він стирає межу між внутрішньодержавною і міжнародною передачею інформації [2]. Так, Інтернет-адреси, що підтримуються мережею, нематеріальні, і навіть адреси сайтів, які містять URL-індикатори країни походження, наприклад, "ua", не обов'язково мають бути точними. В той же час, електронні сигнали, що передаються засобами електричного зв'язку, зберігаються не на віртуальних, а на фізичних носіях, які можуть знаходитися на території певної держави, сигнал, що проходить по певних мережах, акумулюється на серверах, які переміщаються у фізичному просторі й також відносяться до юрисдикції певної держави [2].

Вчинення будь-яких дій з електронними даними, що знаходяться за межами держави, навіть з віддаленого комп'ютера, має кваліфікуватися як порушення державного суверенітету країни, на території якої ці дані зберігаються (пересилаються). При цьому правоохоронці, що діють у кіберпросторі, самі інколи не можуть визначити, чи перетнули вони кордон, чи

ні [6]. У таких випадках кримінальне переслідування злочинця стає неможливим без міждержавного співробітництва. Така особливість мережі Інтернет ставить науку і практику перед необхідністю узгодженого міжнародного підходу на різних рівнях. Адже традиційні угоди про взаємну правову допомогу були створені в часи, коли для збору доказової інформації в іноземній державі правоохоронцям необхідно було фізично перетинати кордони (існувала необхідність безпосередньої присутності), а саму інформацію фізично переміщати з однієї країни в іншу [5].

Проте, сьогодні все більше юристів схиляється до думки, що один із напрямів вирішення проблеми кримінальної юрисдикції у цій сфері полягає у наданні кіберпростору, що має транскордонний характер (інституціональним втіленням якого є мережа Інтернет), правового статусу міжнародної території, аналогічної територіям спільного користування [2, 6]. Зокрема, Д. Менте пропонує вважати Інтернет територією, на яку не поширюється суверенітет окремої держави (космічний простір, нейтральні води, Антарктида тощо) [6]. Як зазначав Г. Кельзен, територія – це не земля (її частина), це образний вираз, що позначає певне якісне право, національний юридичний порядок [6]. Така позиція виглядає досить слушною, і в якості прикладу нормативного закріплення екстериторіального статусу кіберпростору можна навести визначення Верховного Суду США: унікальний носій, який не знаходиться на певній території, але доступний кожному в будь-якій точці світу через Інтернет [2, 6]. У той же час, вказане питання із юридичної площини переходить в політичну, і потребує додаткових зусиль в активізації міждержавного діалогу.

Цілком логічно, що розвиток новітніх технологій (швидкість з'єднання, відсутність кордонів) робить кіберпростір дуже зручним для розвитку специфічних прав і можливостей для працівників підрозділів боротьби з кіберзлочинністю. Вбачається, що сучасна адекватна відповідь на протиправне використання кіберпростору організованою злочинністю повинна ґрунтуватись на розвитку відповідних процедурних повноважень правоохоронних органів у зборі доказів у кіберпросторі. Один із таких напрямів розв'язання вказаних проблем вбачається у постановці проблеми транскордонного доступу (ст. 32 Конвенції).

В юридичній літературі під транскордонним доступом розуміють обшук у комп'ютерних мережах (середовищі для зберігання комп'ютерних даних) за кордоном з метою виявлення і вилучення необхідної для кримінального провадження комп'ютерної інформації [5, 7]. Однією з особливостей Конвенції по боротьбі з кіберзлочинністю є те, що в ній пропонується виходити з того положення, що головна роль у регулюванні процесу розслідування комп'ютерних злочинів належить національному законодавству. Слід наголосити, що Україна проголошує себе правовою державою (ст. 1 Конституції України), а це надає пріоритетного значення саме право-

вим формам і механізмам організації діяльності апарату держави, і, в першу чергу, правоохоронних органів. І якщо внутрішнім правом України не передбачено конкретні повноваження на пошук доказів у електронному середовищі, то така Україна буде не в змозі не тільки адекватно реагувати на прохання про надання правової допомоги, але й наступально протидіяти організованій злочинності у кіберпросторі. Наприклад, чинний КПК не містить положення, які дають змогу використовувати докази в електронній формі.

Як відмічає В. М. Бутузов, в Україні існує нормативна невідповідність між завданнями, покладеними на спецпідрозділи по боротьбі з кіберзлочинністю, і наданні їм повноваження у цій сфері. Адже протидія кіберзлочинності повинна передбачати не тільки захист від загроз у кіберпросторі, а й активний вплив на джерела цих загроз. Тож удосконалення правового регулювання діяльності правоохоронних органів України з протидії організованій кіберзлочинності зумовлює необхідність імплементації до вітчизняного законодавства процедурних положень Конвенції по боротьбі з кіберзлочинністю [8, с. 251, 253].

Виходячи з таких позицій, транскордонний доступ до комп'ютерних даних треба сприймати як реалізацію (за допомогою інформаційних технологій) владних повноважень правоохоронних органів однієї Сторони у здійсненні доступу (отриманні) необхідних даних, обробка яких здійснюється у кіберпросторі, що має транскордонний характер на підставі законної і добровільної згоди особи (наприклад, адміністратора ресурсу), яка має законні повноваження розкривати дані, без застосування традиційних процедур взаємної правової допомоги. Тобто, державі не потрібно одержувати дозвіл іншої Сторони, коли вона діє відповідно до свого національного законодавства. Під обробкою слід розуміти виконання будь-якої однієї або декількох операцій з комп'ютерними даними: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання.

Власне мова йде не про публічно доступні (відкрите джерело) комп'ютерні дані, що доступні будь-яким користувачам, і власнику цих даних про це добре відомо. Доступ (отримання) таких даних регламентується п. a ст. 32 Конвенції по боротьбі з кіберзлочинністю і не викликає дискусій щодо необхідності застосування інституту міжнародної правової допомоги. В той же час, п. b. ст. 32 Конвенції передбачає доступ (отримання) даних за кордоном, які особа хоче зберегти у таємниці (наприклад, за згодою адміністратора ресурсу, який зареєстровано на сервері, розташованого в межах іноземної юрисдикції, оперативні працівники здійснюють оперативний огляд змісту приватної електронної скриньки або за допомогою автентифікаційних даних отримують доступ до профілю користувача, зареєстрованого на сервері, розташованому за кордоном, тощо).

При цьому, на думку А. Г. Волеводза і Т. Б. Світова, залишаються відкритими питання: 1) можливість доступу до даних без отримання згоди користувача чи власника, але з наступним обов'язковим повідомленням останніх або компетентних органів держави, де знаходиться комп'ютерна система чи дані; 2) відсутність регулювання механізму відмови у транскордонному доступі особі, яка володіє законним правом на управління комп'ютерною системою і даними, що в ній зберігаються; 3) порядок оскарження рішення про збирання комп'ютерних даних при транскордонному доступі; 4) захист конфіденційності інформації, отриманої вказаним вище способом; 5) судовий та відомчий контроль національних судів і компетентних органів за законністю дій іноземних органів [9].

Конвенцією по боротьбі з кіберзлочинністю передбачено необхідність забезпечити належний баланс між законодавчим визначенням повноважень правоохоронних органів, достатніх для ефективної боротьби з кіберзлочинами, і повагою до основних прав людини, в т. ч. і права на приватність. Тому відповіді на вищеназвані питання перебувають у площині дотримання вітчизняним законодавцем при імплементації норм Конвенції міжнародних стандартів з прав людини, визначених міжнародними договорами, які є частиною національного законодавства України (ст. 9 Конституції України), відповідності вказаних змін правам і свободам в інформаційній сфері (ст.ст. 31, 32, 34 Конституції України) та забезпечення їх захисту (ст. 55 Конституції України). Це також і питання міждержавних угод щодо винайдення "ціни", яку суспільство готове сплатити за безпеку в телекомунікаційному просторі при розробці процедурних положень з розкриття і розслідування кіберзлочинів і визначення повноважень спецпідрозділів по боротьбі з кіберзлочинністю.

Вбачається, що імплементацію до вітчизняного законодавства положень ст. 32 Конвенції по боротьбі з кіберзлочинністю слід розглядати як надання специфічних прав і можливостей спецпідрозділів по боротьбі з кіберзлочинністю з реалізації оперативно-розшукових заходів у е-середовищі. При цьому саму ст. 32 Конвенції по боротьбі з кіберзлочинністю варто доповнити процедурними положеннями, за аналогією викладеними у Конвенції Європейського Союзу про взаємну правову допомогу в кримінальних справах між країнами-учасницями Європейського Союзу 2000 р.

Остання передбачає два шляхи отримання відомостей про повідомлення, які передаються по мережі електричного зв'язку з проходженням через іноземні території: 1) в порядку надання взаємної правової допомоги з письмового доручення у випадках, коли запитуюча сторона без технічної підтримки запитуваної сторони самостійно не може отримати до них доступ; 2) без направлення міжнародного доручення про взаємну правову допомогу, якщо держава без технічної під-

тримки іноземних компетентних органів самостійно здійснює за кордоном збирання доказів у вигляді відомостей про повідомлення електрозв'язку [7].

Тобто, в одному з випадків передбачається екстериторіальна кримінально-процесуальна юрисдикція та підкреслюється примусовий характер оперативно-розшукових заходів або негласних слідчих (розшукових) дій, що не потребує направлення міжнародного доручення про взаємну правову допомогу. На сьогодні такий підхід є певним обмеженням державного суверенітету, тому для його реалізації необхідна згода відповідної держави. З огляду на це, державам варто укладати угоди, в яких передбачати обов'язкове інформування компетентних органів про всі випадки прямого транскордонного доступу до конфіденційних даних.

В умовах, коли питання встановлення факту поширення внутрішньодержавних правових норм і відносини в Інтернет просторі на міжнародному рівні залишаються не вирішеними, вітчизняним правоохоронцям слід керуватись чинними принципами міжнародного права, конституційним принципом дозволеності діянь, не заборонених законодавством, ст.ст. 2, 8, 31, 32 Конституції України та чинним законодавством.

Висновки дослідження і перспективи подальших розвідок у даному напрямі. Міждержавні механізми пошуку доказів у електронному середовищі існують, потрібен лише єдиний підхід до внутрішньодержавних процедурних положень щодо оперативного доступу та отримання необхідних даних у глобальних мережах електрозв'язку. При імплементації до вітчизняного законодавства положень ст. 32 Конвенції по боротьбі з кіберзлочинністю слід забезпечити відповідність між завданнями, покладеними на спецпідрозділи по боротьбі з кіберзлочинністю, з наданими їм повноваженнями у цій сфері.

В перспективі подальші розвідки доцільно проводити у напрямі вироблення єдиних підходів до процедури отримання законної і добровільної згоди особи, яка має законне право дозволити розкриття конфіденційних даних при транскордонному доступі до застосування технічних можливостей для руйнування систем захисту інформації з метою одержання доказової інформації проти членів злочинних угруповань, що зберігається у е-середовищі, без направлення письмового доручення про надання правової допомоги.

Список використаних джерел

1. Золотий час Carderplanet / [Електронний ресурс] – Режим доступу : http://easy-code. com. ua/2010/11/zolotij-chas-carderplanet/.

2. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій [Електронний ресурс] / І. В. Європіна. – Режим доступу : http://archive. nbuv. gov. ua/portal/Soc_Gum/Vaau/2010_3/text/10eivnit. pdf.

3. Зозуля Є. В. Діяльність органів державної влади та управління України щодо нормативно-правового та організаційного забезпечення міжнародного співробітництва у боротьбі з кіберзлочинністю / Є. В. Зозуля // Наука. Релігія. Суспільство. – 2011. – № 2. – С. 54–60.

4. Про результати відрядження працівників УБК МВС України до Австрії: Звіт заступникові Міністра внутрішніх справі України від 12 листоп. 2012 р.

5. Смирнов М. І. Процесуальні особливості застосування нових форм взаємної правової допомоги по кримінальних справах [Електронний ресурс] / М. І. Смирнов. – Режим доступу :
http://univer. km. ua/visnyk/658. pdf.

6. Манжай О. Використання кіберпростору в ОРД [Електронний ресурс] / О. Манжай. – Режим доступу:
www. nbuv. gov. ua/portal/…/PB-4_48. pdf.

7. Пашковський М. І. Співробітництво поліцій і судових органів в сфері кримінального судочинства відносно транснаціональних злочинів: модель Європейського Союзу [Електронний ресурс] / М. І. Пашковський. – Режим доступу :
http://inter. criminology. org. ua/? p=1617.

8. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : КИТ, 2010. – 408 с.

9. Цимбал П. Правові аспекти міжнародного співробітництва у боротьбі з комп'ютерною злочинністю [Електронний ресурс] / П. Цимбал, Н. Постіл. – Режим доступу :
http://www. asta. edu. ua/vidan/nau_visn/3(25)/Pravo/ZIP/Tsumbal. zip.

В статье рассмотрены проблемы применения трансграничного доступа к компьютерным данным как формы взаимной правовой помощи по противодействию организованной киберпреступности.

In this article the problems of interstate access to computer data as a form of inter judicial assistant against organized cybercrimes are investigated.

Стаття надійшла до редакції журналу 11 березня 2013 року.