КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНЕ ПРАВО ТА КРИМІНАЛІСТИКА

АХТИРСЬКА Н. М.,
кандидат юридичних наук,
доцент, головний науковий співробітник
відділу науково-методичного забезпечення
діяльності
*(Вища кваліфікаційна комісія суддів України
та Вища рада юстиції Національної школи
суддів України)*

УДК 343.18

ЗАКОНОДАВЧЕ ВРЕГУЛЮВАННЯ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ У СПРАВАХ, ПОВ'ЯЗАНИХ З ІНТЕРНЕТОМ

У статті аналізуються конвенційні норми та положення чинного законодавства щодо посилення взаємодії й міжнародної співпраці в боротьбі з кіберзлочинністю. Запропоновано переглянути положення законів про ратифікацію Конвенції про боротьбу з кіберзлочинністю та Додатковий протокол до неї щодо можливості їх ратифікації без застережень.

Ключові слова: *кіберзлочинність, Інтернет, юрисдикція, міжнародне співробітництво під час кримінального провадження.*

В статье анализируются конвенционные нормы и положения действующего законодательства касательно взаимодействия и международного сотрудничества в борьбе с киберпреступностью. Внесено предложение о пересмотре положений законов Украины о ратификации Конвенции против киберпреступности и Дополнительного протокола к ней на предмет возможности их ратификации без оговорок.

Ключевые слова: *киберпреступность, Интернет, юрисдикция, международное сотрудничество в уголовном судопроизводстве.*

There are analyzed conventional norms and positions of current legislation concerning strengthening of cooperation and international cooperation in a fight with cybercrime. Also it is suggested to reconsider positions of laws of Ukraine about ratification of Convention against cybercrime and Additional protocol to it for the purpose possibility of their ratification without reservations.

Key words: *cybercrime, Internet, jurisdiction, international cooperation in criminal proceedings.*

Вступ. Глобальна мережа Інтернет, як і будь-яке явище, супроводжується низкою як позитивних наслідків (доступ до інформації, дистанційне навчання, швидкість повідомлень), так і негативних результатів і ризиків, у тому числі вчиненням за допомогою всесвітньої мережі злочинів. Аналітики американського Центру стратегічних та міжнародних досліджень (CSIS) стверджують, що світова економіка щорічно втрачає від кіберзлочинів 445 мільярдів доларів США [1]. З урахуванням цієї специфіки злочинного механізму ускладнюється процес одержання доказів у зв'язку з їх неочевидністю, швидкоплинністю, нестійкістю й територіальною недоступністю (за межами держави). Незважаючи на наяв-

ність кримінальної відповідальності за вчинення злочинів із використанням інформаційних технологій, Україна зазнає серйозної загрози з боку кіберзлочинців, що зумовлює потребу посилення міжнародної співпраці під час кримінального провадження. Відповідно до Резолюції наради Ради Європи від 12–14 листопада 2014 р., країни мають проревізувати чине законодавство та забезпечити механізм співпраці під час кримінального провадження в цій категорії кримінальних правопорушень [2].

Низький рівень виявлення кіберзлочинів, притягнення винних до відповідальності потребує виявлення законодавчих прогалин, що сприяють цьому, а також вирішення питань юрисдикції судів щодо злочинів, які виходять за межі територіальності.

Постановка завдання. Метою статті є аналіз конвенційних норм і положень чинного законодавства щодо посилення взаємодії й міжнародної співпраці в боротьбі з кіберзлочинністю.

Результати дослідження. Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. закріпила положення про «необхідність спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва» [3]. Усвідомлюючи глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, ураховуючи ризики того, що комп'ютерні мережі та електронна інформація може також використовуватися для здійснення кримінальних правопорушень, і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатися й передаватися такими мережами, Україна 23 листопада 2001 р. підписала цей міжнародний документ, який 07 вересня 2005 р. був ратифікований (набув чинності 01 липня 2006р.). Однак варто зазначити, що Україна ратифікувала Конвенцію із застереженнями та заявами [4]. Відповідно до п. 1 ст. 6 Конвенції, кожна Сторона вживає такі законодавчі й інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це: a. виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином: i. пристроїв, включаючи комп'ютерні програми, створені або адаптовані передусім з метою вчинення будь-якого зі злочинів, перерахованих у ст. ст. 2–5 (незаконний доступ; нелегальне перехоплення втручання в дані; втручання в систему); ii. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у ст. ст. 2–5; b. володіння предметом, перерахованим у підпунктах a. і або ii, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у ст. ст. 2–5. Сторона може передбачити в законодавстві, що для встановлення кримінальної відповідальності необхідно володіти певною кількістю таких предметів. Законом про ратифікацію Конвенції Україна залишила за собою право не застосовувати цей пункт у частині встановлення кримінальної відповідальності.

Як зазначено в п. 1 ст. 9 Конвенції, кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення без права на це таких дій: a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем; b. пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем; c. розповсюдження або передавання дитячої порнографії за допомогою комп'ютерних систем; d. здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; e. володіння дитячою порнографією в комп'ютерній системі чи на комп'ютерному носії інформації. Незважаючи на особливу небезпечність дитячої порнографії та її поширення в суспільстві, Україна залишила за собою право не застосовувати повністю підпункти 1.d та 1.e ст. 9 Конвенції.

Відповідно до п. 7. a. ст. 24 Конвенції, кожна Сторона під час підписання або передавання на зберігання своєї ратифікаційної грамоти чи документа про прийняття, схвалення чи приєднання повідомляє Генеральному секретарю Ради Європи назви й адреси всіх компетентних органів, які відповідають за надсилання чи отримання запитів про екстрадицію або тимчасовий арешт у випадку відсутності договору. В Україні органами, на які покладаються

повноваження, згідно з п. 7 ст. 24 Конвенції, є Міністерство юстиції України (щодо запитів судів) і Генеральна прокуратура України (щодо запитів органів досудового слідства).

Згідно з п. 1 ст. 35 Конвенції, кожна Сторона призначає орган для здійснення контактів цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних із комп'ютерними системами й даними, або з метою збирання доказів в електронній формі, що стосуються кримінального правопорушення. Така допомога включає сприяння або, якщо це дозволяється її внутрішньодержавним законодавством і практикою, пряме: a. надання технічних порад; b. збереження даних відповідно до ст. ст. 29 «Термінове збереження комп'ютерних даних, які зберігаються» і 30 «Термінове розкриття збережених даних про рух інформації»; c. збирання доказів, надання юридичної інформації й установлення місцезнаходження підозрюваних. В Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних із комп'ютерними системами й даними переслідуваних осіб, котрі обвинувачуються в учиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України [5].

Задля ефективного дотримання всіх прав людини без будь-якої дискримінації або розділення, як це гарантується європейськими та іншими міжнародними документами; будучи переконані, що дії расистського і ксенофобного характеру є порушенням прав людини та загрозою верховенству права й демократичній стабільності; уважаючи, що національне та міжнародне право має забезпечувати адекватну правову реакцію на пропаганду расистського і ксенофобного характеру, яка здійснюється через комп'ютерні системи, 20 січня 2003 р. був підписаний Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського і ксенофобного характеру, учинених через комп'ютерні системи [6]. При цьому варто зазначити, що, визнаючи загрозу вказаного явища, Україна ратифікувала цей протокол із заявами та застереженнями [7]. Відповідно до ст. 6, кожна Сторона вживає таких законодавчих й інших заходів, які можуть бути необхідними для визнання таких дій кримінальними правопорушеннями в її національному законодавстві, у разі умисного вчинення без права на це: розповсюдження або іншим чином надання громадськості доступу через комп'ютерні системи до матеріалу, який заперечує, значно мінімізує, схвалює або виправдовує дії, які є геноцидом або злочинами проти людства, як це визначено в міжнародному праві й заключними та обов'язковими рішеннями Міжнародного військового трибуналу, основаного згідно з Лондонською угодою від 08 серпня 1945 року, або будь-якого іншого міжнародного суду, основаного відповідними міжнародними документами, юрисдикція якого визнана такою Стороною. У Законі про ратифікацію Україна заявила, що вона вимагатиме, щоб заперечення чи значна мінімізація, про які йдеться в п. 1 цієї статті, були вчинені з наміром підбурити до ненависті, дискримінації чи насильства проти будь-якої особи чи групи осіб на підставі ознак раси, кольору шкіри, національного чи етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій.

Незважаючи на значне посилення активності екстремістськи налаштованих угруповань, збільшенням кількості потерпілих серед представників інших національностей (іншого віросповідання та кольору шкіри), правоохоронними органами приховується цей вид злочину, оскільки, як свідчить практика, відкриваються кримінальні провадження за статтею Кримінального кодексу України (далі – КК України), яка передбачає відповідальність за хуліганство. Підтвердженням тому є статистичні дані Державної судової адміністрації України: усього за 2006–2014 рр. судами України було розглянуто лише 20 кримінальних проваджень за ст. 161 КК України, з постановленням вироку лише 8, закриттям – 7; поверненням на додаткове розслідування – 5; засуджено 8 осіб, виправдано 2 особи [8].

На нашу думку, з урахуванням кампанії щодо обговорення проекту Закону України «Про боротьбу з кіберзлочинністю» доцільно розглянути можливість ратифікації Конвенції та Додаткового протоколу без застережень шляхом унесення змін до відповідних законів.

Представники банківського сектора наголошують на загрозі незаконного отримання готівкових коштів за підробними платіжними картками іноземних банків-емітентів, що у професійній термінології здобуло назву «білий пластик». У дослідженні, що відобразило кількісний обсяг проблеми в загальному розрізі шахрайських операцій із платіжними інструментами, взяли участь банки-члени Асоціації ЄМА, які представляють понад 90% ринку емісії платіжних інструментів. Було встановлено, що частка іноземних емітентів, за підробленими картками яких здійснювались шахрайські транзакції в АТМ мережі зазначених банків, на території України становить 86,6%, що свідчить про суттєву обізнаність зловмисників щодо існування прогалини у правовому регулюванні протидії кіберзлочинності [9]. Проблеми правової кваліфікації використання «білого пластику» в банкоматній мережі України лежать передусім у площині відсутності єдиного підходу в слідчих і судових органів до кваліфікації цього злочинного вияву. Звідси – неоднаковість підходів до застосування кримінального законодавства загалом, у результаті чого порушується насамперед конституційний принцип рівності всіх, у т. ч. і перед законом, і судом (ст. 24 Конституції України). На практиці складається ситуація, коли за відсутності жодного роз'яснювального акта вищих органів судової влади за тотожні склади злочинів карають за різними статтями КК України виходячи із суб'єктивного розуміння слідчих і суддів суті правовідносин у цій сфері. Підтвердженням є наявність вироків, що набрали законної сили, одночасно за ст. 200, ч. 3 ст. 190 КК України, а також за сукупністю у варіаціях за ст. 200 та ч. 3 ст. 190 КК України, а інколи й іншими суміжними статтями КК України. РГ було зібрано та проаналізовано такі судові вироки, а також заяви банків до МВС України. Було зібрано 32 заяви за ст. 200, ч. 3 ст. 190, ст. ст. 361-1, 231 КК України, із них виключно щодо «білого пластика» – 22, з них – відмов у порушенні кримінально справи – 10. Тобто, близько половини (45,45%) заявлених злочинів навіть не підлягали розгляду.

Одним із дискусійних питань у цьому аспекті є питання юрисдикції судів у провадженнях, пов'язаних з Інтернетом. Варто одразу зауважити, що юрисдикція – установлена законодавством сукупність повноважень відповідних органів державної влади та органів місцевого самоврядування розглядати й вирішувати правові спори і справи про правопорушення, давати правову оцінку діянням осіб або інших суб'єктів права з погляду їх правомірності або неправомірності, застосовувати санкції до правопорушників [10, с. 490]. Цим терміном також визначають повноваження суду розглядати й вирішувати справи. Крім того, цей термін використовується для окреслення території, у межах якої суд може здійснювати свою юрисдикцію. Юрисдикція – це складова суверенітету, а отже, вона обмежена географічними кордонами. Тому особливого значення набуває це поняття у провадженнях, пов'язаних з Інтернетом, оскільки Інтернет-транзакції й Інтернет-публікації не знають кордонів. Іншими словами, такі справи, як правило, містять транскордонний елемент. У зв'язку з цим виникають питання: за яких обставин суд може здійснювати юрисдикцію, якщо особа своїми діями в Інтернеті завдала шкоду іншій особі й заяву про злочин або цивільний позов подано в одній країні, а відповідач перебуває чи проживає в іншій країні? В окремих випадках це питання належить до вирішення національними судами, які вирішують його на підставі принципів міжнародного права. Європейський суд з прав людини не розглядає ці питання по суті. Це підтверджується нещодавнім рішенням Суду у справі Премініни проти Росії. Як свідчить практика, європейський суд з прав людини розглянув лише кілька справ, де питання юрисдикції поставали в контексті Інтернету (Перрін проти Сполученого Королівства). Заявник, громадянин Сполученого Королівства, що проживав у Франції, опублікував в Інтернеті статтю непристойного характеру, за що його засудили до позбавлення волі. Сайт, де було опубліковано статтю, управлявся й контролювався американською компанією, що діяла відповідно до місцевого законодавства, а заявник був мажоритарним акціонером компанії. Європейський суд з прав людини погодився з Апеляційним судом Британії, що якщо національні суди розглядають справи про поширення інформації лише тоді, коли місце опублікування матеріалу потраплятиме під їхню територіальну юрисдикцію, то видавці публікуватимуть свої матеріали там, де ймовірність притягнення їх до відповідальності за

опублікування цих матеріалів є малою. Далі суд зазначив, що оскільки заявник проживає у Сполученому Королівстві, то він не може стверджувати, що не мав розумного доступу до місцевого законодавства. Цікавою є думка суду стосовно пропорційності призначеного покарання. Він зазначив, що, хоча в інших країнах поширення таких фотографій може бути визнано правомірним, це не означає, що коли Уряд-відповідач забороняє поширювати знімки і притягає заявника до відповідальності, то він перевищує надані йому межі свободи розсуду. У підсумку суд вирішив, що заява є явно необґрунтованою в розумінні п. 3 ст. 35 Конвенції [11].

Висновки. Отже, у Законі України «Про боротьбу з кіберзлочинністю» або в Кримінальному процесуальному кодексі України варто окремо визначити питання юрисдикції. Такий підхід буде сприяти ефективній боротьбі з кіберзлочинністю й ефективному функціонуванню міжнародного співробітництва у кримінальних питаннях, оскільки Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами й даними шляхом установлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями через сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, укладення домовленостей щодо швидкого й надійного міжнародного співробітництва.

Список використаних джерел:

1. Мировая экономика теряет из-за киберпреступности $ 445 млрд ежегодно [Электронный ресурс]. – Режим доступа : http://rtr.md/novosti/hi-tech/mirovaya-ekonomika-teryaet-iz-za-kiberprestupnosti-445-mlrd-ezhegodno-issledovanie.

2. Возможности борьбы с информационной преступностью в государствах «Восточного партнерства» : Резолюция совещания Совета Европы от 12–14 ноября 2014 г. [Электронный ресурс]. – Режим доступа : http://conventions.coe.int/Treaty/RUS/Treaties/Html/185.htm.

3. Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. // Офіційний вісник України. – 2007. – № 65. – С. 107. – Ст. 2535.

4. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07 вересня 2005 р. № 2824-IV // Урядовий кур'єр. – 2005. – № 185.

5. Про внесення зміни до Закону України «Про ратифікацію Конвенції про кіберзлочинність» : Закон України від 21 вересня 2010 р. № 2532-VI // Голос України. – 2010. – № 192.

6. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28 січня 2003 р. // Офіційний вісник України. – 2010. – № 56. – С. 73. – Ст. 1920.

7. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України 21 липня 2006 р. № 23-V // Офіційний вісник України. – 2006. – № 31. – С. 29. – Ст. 2202.

8. Інформація про стан розгляду кримінальних справ за статтею 161 Кримінального кодексу України за 2006–2014 рр. [Електронний ресурс]. – Режим доступу : http://court.gov.ua/sudova_statystyka/.

9. Щодо необхідності роз'яснення судам особливостей розгляду справ за злочинами, що вчиняються з платіжними інструментами // Лист Української міжбанківської асоціації членів платіжних систем «ЄМА» до Національної школи суддів України від 16 квітня 2015 р.

10. Педько Ю.С. Юрисдикція. Юридична енциклопедія / Ю.С. Педько. – К. : Українська енциклопедія ім. М.П. Бажана, 2004.

11. Інтернет: практика Європейського суду з прав людини. Дослідницьке управління Європейського суду з прав людини, 2011.