УДК 343.13

ПРАВОВА ОСНОВА ОТРИМАННЯ ІНФОРМАЦІЇ З МЕРЕЖІ ІНТЕРНЕТ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Школьніков В. І.,
здобувач наукової лабораторії з проблем досудового розслідування
Навчально-наукового інституту № 1
Національної академії внутрішніх справ

У статті проаналізовано нормативно-правові акти, що стосуються порядку отримання інформації з мережі Інтернет у кримінальному проваджені. Визначено рівні нормативно-правового регулювання порядку отримання інформації з мережі Інтернет у кримінальному проваджені. Визначено прогалини в кримінальному процесуальному законодавстві щодо отримання інформації з мережі Інтернет.

В статье проанализированы нормативно-правовые акты, касающиеся порядка получения информации из сети Интернет в уголовном производстве. Определены уровни нормативно-правового регулирования порядка получения информации из сети Интернет в уголовном производстве. Определены пробелы в уголовном процессуальном законодательстве относительно получения информации из сети Интернет.

Legal acts concerning the procedure of obtaining information from the Internet in criminal proceedings have been analyzed. Levels of legal regulation of the order of obtaining information from the Internet in criminal proceedings have been defined. The gaps in the criminal procedural law concerning the procedure of obtaining information from the Internet has been identified.

Ключові слова: кримінальний процес, правова основа, інформація, мережа Інтернет.

Постановка проблеми. Стрімкий розвиток інформаційних технологій призводить до появи нових способів учинення кримінальних правопорушень, зокрема в мережі Інтернет. Інформація в Інтернет-середовищі може свідчити про факт учинення певного правопорушення (яке не обов'язково має належати до категорії кіберзлочинів), містити відомості про його сліди та шкідливі наслідки [1, с. 12].

На сучасному етапі діяльності вітчизняних правоохоронних органів існує проблема, яка полягає в правильній процедурі отримання інформації, що міститься в мережі Інтернет.

По-перше, нерозуміння слідчим основ структури та організації мережі Інтернет може призвести до порушення завдань кримінального провадження, визначених ст. 2 Кримінального процесуального кодексу України (далі – КПК України).

По-друге, безмежність та відсутність певних територіальних обмежень в обігу інформації в мережі Інтернет потребує від слідчого досконалих знань у сфері міжнародного співробітництва та законодавства тієї держави, де знаходиться володілець потрібної інформації.

Тому виникає проблема в розробленні наукових рекомендацій із пошуку, виявлення та фіксації інформації з мережі Інтернет у кримінальному провадженні. Одним із перших завдань повинно стати обґрунтування необхідності зміни практики, що склалася під час досудового розслідування кримінальних правопорушень, та яка полягає в неправильному правозастосуванні положень КПК України.

Теоретичним підґрунтям наукового дослідження стали праці вітчизняних і зарубіжних учених, які вівчали різні аспекти отримання інформації з мережі Інтернет, це, зокрема, Н.М. Ахтирська, О.В. Малахова, Ю.Ю. Орлов, С.В. Самойлов, В.Г. Уваров, Є.С. Хижняк, Д.М. Цехан, С.С. Чернявський та ін. Натомість відсутність системних теоретичних напрацювань саме з питання правової регламентації порядку отримання інформації з мережі Інтернет у кримінальному провадженні зумовлює необхідність проведення такого дослідження.

Мета статті – аналіз правових основ отримання інформації з мережі Інтернет з метою зміни правозастосовної практики діяльності правоохоронних органів під час досудового розслідування кримінальних правопорушень.

Виклад основного матеріалу. Правова основа – це сукупність вихідних положень нормативно-правових актів, які регламентують діяльність конкретних суб'єктів правозастосування або суспільні відносини загалом.

Правову основу отримання інформації з мережі Інтернет у кримінальному провадженні становлять чинні нормативно-правові акти, які регламентують відносини між судом, слідчим суддею, прокурором, органами досудового розслідування, оперативними підрозділами та громадянами, а також підприємствами, установами й організаціями з питань отримання інформації, що має доказове або орієнтуюче значення.

Особливість обігу інформації в мережі Інтернет полягає в тому, що така інформація знаходиться, як правило, у володінні, утриманні або користуванні конкретних підприємств, установ або організацій, наприклад, в адміністрації таких соціальних мереж, як Facebook, Twitter, LinkedIn, Instagram тощо.

А тому, аналізуючи правові основи отримання інформації з мережі Інтернет у кримінальному провадженні, доцільно виділити такі рівні нормативно-правового регулювання цієї діяльності:

1 – норми міжнародно-правового характеру;

2 – конституційні норми;

3 – закони України;

4 – підзаконні нормативно-правові акти.

До першого рівня слід віднести Загальну декларацію прав людини 1948 року, де в статті 12 указано, що «ніхто не може зазнавати довільного втручання в його особисте і сімейне життя, довільного посягання на недоторканність його житла, таємницю його кореспонденції чи на його честь і репутацію. Кожна людина має право на захист закону від такого втручання чи від такого посягання» [2]. Це початкове положення знайшло своє відображення і було розвинене в статті 17 Міжнародного Пакту про громадянські і політичні права, прийнятого 16 грудня 1966 року Генеральною Асамблеєю Організації Об'єднаних Націй [3], і в статті 8 Європейської декларації про захист прав людини і основних свобод [4]. Ці міжнародно-правові акти становлять основу захисту основоположних прав людини від незаконного втручання та є складовою частиною кримінального процесуального законодавства України відповідно до статті 1 КПК України.

Також 07 вересня 2015 року Україною була ратифікована Конвенція Ради Європи про кіберзлочинність [5], згідно з якою кожна держава, що підписала цей міжнародно-правовий документ, зобов'язана вжити таких заходів законодавчого та іншого характеру, які можуть знадобитися для збору доказів у кримінальних провадженнях в електронній формі. Додатково Конвенція надає право збирати комп'ютерні данні в онлайн-режимі та з відкритих джерел без згоди іншої сторони, встановлює обов'язок широкого співробітництва між країнами з питань збору електронних доказів тощо. Але слід відмітити, що на практиці країни-учасниці не дотримуються положень Конвенції, однією з головних причин цього є різна правова регламентація порядку розслідування кримінальних правопорушень на території країн-учасниць.

Тому в питанні отримання інформації з мережі Інтернет важливу роль відіграє міжнародне співробітництво. У даному контексті слід погодитися з думкою Ю.М. Чорноус про те, що до правових основ міжнародного співробітництва в діяльності з розслідування злочинів відносяться міжнародні договори та міжнародні угоди України [6, с. 221]. Тобто велику роль у питанні отримання інформації з мережі Інтернет відграють також міжнародні угоди України.

Відповідно, другим рівнем нормативно-правового регулювання є Конституція України [7]. Так, ст. 30 Конституції України захищає недоторканність житла (територіальну приватність), ст. 31 – таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (комунікаційну приватність), ст. 32 передбачає заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (інформаційна приватність), а ст. 28 передбачає заборону піддавати особу без її вільної згоди медичним, науковим чи іншим дослідам (фізична приватність).

До третього рівня слід віднести КПК України, норми якого необхідно поділити на такі групи:

І. Загального призначення, які визначають загальні положення отримання інформації з мережі Інтернет у кримінальному провадженні, порядок визнання такої інформації доказом у кримінальному провадженні.

У контексті подальшого наукового дослідження цікавими та такими, які потребують змін, є правові норми, що стосуються статті 99 КПК України.

Необхідно погодитися з думками Ю.Ю. Орлова та С.С. Чернявського з приводу того, що буквальне тлумачення тексту ст. 99 КПК України дає підстави для висновку, що «електронні носії інформації» потрібно трактувати як будь-які електронні носії. Такі носії можуть бути вбудовані в комп'ютерні пристрої, підключені до інформаційної мережі [8, с. 14].

Натомість сучасний розвиток інформаційних технологій зумовлює потребу у визнанні окремим джерелом доказів саме електронну інформацію, особливо якщо остання знаходиться в обігу в мережі Інтернет. Це пояснюється тим фактом, що встановити першоджерело походження такої інформації є вкрай трудним завданням, особливо якщо така інформація постійно передається з одного веб-ресурсу на інший. Крім того, гостро постає питання того, що володільці, користувачі або утримувачі

такої інформації знаходяться за кордоном. Наслідком цього є неможливість слідчому отримати таку інформацію, наприклад, шляхом тимчасового доступу до електронної інформаційної системи;

II. Досудового розслідування в частині регламентації порядку проведення слідчих (розшукових) та негласних слідчих (розшукових) дій.

Так, інформація з мережі Інтернет може бути отримана під час обшуку (ст. 234), тимчасового доступу до електронних інформаційних систем як заходу забезпечення кримінального провадження (ст. 159), а також під час зняття інформації з електронних інформаційних систем (ст. 264).

У науковій літературі та в практичній діяльності розповсюдженою є думка про те, що огляд як слідча (розшукова) дія є процесуальним засобом отримання інформації з мережі Інтернет [9–13]. На наше переконання, така практика порушує завдання та засади кримінального провадження з певних причин.

По-перше, огляду веб-сторінки завжди передує пошук конкретної інформації. Такий пошук, як правило, здійснюється з використанням, наприклад, спеціальних формул у Google пошуку (оператори AND, OR тощо), або може навіть використовуватися спеціальне програмне забезпечення, таке як Maltego CE.

Відповідно до ст. 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

У статті 264 КПК України чітко зазначено, що зняття інформації з електронних інформаційних мереж включає:

1) пошук, виявлення і фіксацію відомостей, що містяться в електронній інформаційній системі, або їхніх частин;

2) доступ до електронної інформаційної системи або її частини;

3) отримання таких відомостей без відома її власника, володільця або утримувача.

Відповідно до частини 2 цієї статті не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або їхньої частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. Саме ця частина регламентує здійснення зняття інформації з мережі Інтернет, доступ до якої не обмежується.

По-друге, слідчий здійснює огляд веб-сторінки, яка відображена в певному Інтернет-браузері (Google Chrome, Opera, Microsoft Explorer тощо). Тобто браузер інтерпретує HTML-код конкретної веб-сторінки, а тому слідчий здійснює огляд «зовнішньої сторони», але не знає, що ховається за цією картинкою. У теорії та практиці хакерських атак існує такий тип вразливості, як XSS (англ. Cross Site Scripting – «міжсайтовий скриптинг»). Тобто є можливість у зловмисника змінити структуру HTML-коду веб-сторінки, наприклад, додавши «скрипт», який буде виконувати якусь послідовність дій. Як правило, це переправлення на інший веб-сайт. Але можливо й змінити інформацію, що міститься на веб-сторінці. Тому для слідчого головним завданням є дослідження саме HTML-коду.

Це дуже великий масив даних, які придатні для автоматизованої обробки засобами обчислювальної техніки. На практиці така обробка здійснюється з використанням таких мов програмування, як Python, R.

Тому, на нашу думку, з урахуванням чинних норм Конституції України (ст. 19) та КПК України (ст. 264) доцільніше здійснювати зняття інформації з електронних інформаційних систем, до якої і відноситься мережа Інтернет. Але відсутність практики по застосуванню даної негласної слідчої (розшукової) дії (далі – НС(Р)Д) полягає в порядку засекречення та розсекречення матеріалів проведення зняття інформації з електронних інформаційних систем, яке є часовим бар'єром для слідчого, тим паче судова практика визнає доказом огляд інформації з мережі Інтернет.

Хоча ч. 2 ст. 264 КПК України, яка дозволяє здобувати відомості з електронних інформаційних систем або їхньої частини, доступ до яких не обмежується її власником, володільцем, утримувачем або не пов'язаний з подоланням системи логічного захисту, не потребує ухвали слідчого судді та не порушує приватність спілкування, але відповідно до чинного законодавства існує обов'язок засекречення матеріалів проведення даної НС(Р)Д.

Дане питання є таким, що потребує подальшого наукового дослідження, тому що частина 2 ст. 264 КПК України охоплює таку концепцію, як аналіз відкритих джерел інформації (з англ. Open source intelligence), методики здійснення якої є у вільному доступі в мережі Інтернет.

У цьому контексті слід погодитися з позицією М.Л. Грібова, який пропонує поповнити перелік законодавчо закріплених НС(Р)Д. Вчений уважає за необхідне в системі НС(Р)Д визначити таку дію, як збирання інформації без втручання в приватне спілкування, однією із форм реалізації якої є одержання відкритої інформації в мережі Інтернет. Особливість даних дій, на думку науковця, повинна полягати в збереженні таємниці мети їх проведення та відомчої належності осіб, що їх здійснюють [14].

III. Міжнародного співробітництва під час досудового розслідування.

Окрім КПК України, до третього рівня нормативно-правового регулювання слід віднести такі нормативно-правові акти:

– Закон України «Про електронні документи та електронний документообіг», де в ст. 8 указано, що допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму;

– Закон України «Про оперативно-розшукову діяльність», де зазначається, що оперативним підрозділам для виконання завдань оперативно-розшукової діяльності за наявності передбачених статтею 6 цього Закону підстав надається право здійснювати аудіо-, відеоконтроль особи, зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж згідно з положеннями статей 260, 263–265 КПК України (п. 9 ч. 1 ст. 8);

До четвертого рівня нормативно-правової регламентації порядку отримання інформації з мережі Інтернет слід віднести Інструкцію про організацію проведення НС(Р)Д та використання їхніх результатів у кримінальному провадженні (далі – Інструкція) [15].

Перш ніж перейти до розгляду основних положень Інструкції, необхідно відмітити, що підзаконні нормативно-правові акти повинні містити організаційні процесуальні норми та не розширювати чи звужувати зміст і обсяг конкретних норм кримінального процесуального законодавства.

Так, у п. 1.11.6. Інструкції лише вказано, що зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача (ст. 264 КПК України) полягає в одержані інформації, в тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі.

Натомість більше роз'яснень потребує ч. 2 ст. 264 КПК України, яка регламентує порядок проведення здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.

Висновки. Здійснений аналіз правових основ отримання інформації з мережі Інтернет у кримінальному провадженні доводить всю складність даної сфери наукових досліджень. Характерні ознаки глобальності та інформаційної технологічності даного питання зумовлюють і подальше наукове розроблення рекомендацій, спрямованих на правильне застосування норм кримінального процесуального законодавства. Недосконаліть чинного законодавства та наявність прогалин у порядку отримання інформації з мережі Інтернет у кримінальному провадженні зумовлює необхідність вироблення єдиної стратегії законодавчого вдосконалення порядку отримання такої інформації. Для цього співпраця між правоохоронцями, науковцями та спеціалістами ІТ-сфери є запорукою якісної розробки нового кримінального процесуального законодавства, яке буде відповідати всім вимогам, що впроваджує сучасне інформаційне суспільство.

Література:

1. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. / О.Є. Користін, В.М. Бутузов, С.С. Чернявський та ін. Київ: Скіф, 2012. 736 с.
2. Загальна декларація прав людини від 10 грудня 1948 р. Офіційний вісник України. 2008. № 93. С. 89. Ст. 3103.
3. Д.В. Скринька. Міжнародний пакт про громадянські та політичні права 1966. Українська дипломатична енциклопедія: у 2-х т.; редкол.: Л.В. Губерський (голова) та ін. К.:Знання України, 2004 Т. 2. 812 с.
4. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. Офіційний вісник України. 2006. № 32. Ст. 270.
5. Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. Офіційний вісник України. 2007. № 65. С. 107. Ст. 2535.
6. Чорноус Ю.М. Правова основа міжнародного співробітництва у розслідуванні злочинів. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. 2010. Вип. 1. С. 217–225.
7. Конституція України. Відомості Верховної Ради України (ВВР). 1996. № 30. С. 141. URL: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
8. Орлов Ю.Ю., Чернявський С.С. Електронне відображення як джерело доказів у кримінальному провадженні. Юридичний часопис Національної академії внутрішніх справ. 2017. № 1. С. 12–24.
9. Вирок Богунського районного суду м. Житомира від 14.11.2011 року в кримінальній справі № 1-651/11. URL: http://reyestr.court.gov.ua/Review/52525082
10. Вирок Октябрського районного суду м. Полтава від 07.04.2011 року в кримінальній справі № 1-332/11. URL: http://reyestr.court.gov.ua/Review/15412463
11. Вирок Орджонікідзевського районного суду м. Харкова від 14.09.2016 року в кримінальному провадженні № 1-кп/644/482/15. URL: http://reyestr.court.gov.ua/Review/61312581

12. Хижняк Є.С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. Держава та регіони. Серія «Право». 2017. № 4 (58). С. 80–85.
13. Коваленко А.М. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. Вісник Національної академії правових наук України. 2017. № 1 (88). С. 182–191.
14. Грібов М.Л. Доповнення переліку негласних слідчих (розшукових) дій: практична необхідність та юридична доцільність. Бюлетень Міністерства юстиції України. 2015. № 4. С. 120–126.
15. Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: Інструкція, затверджена наказом ГПУ, МВС, СБУ, АДПС, Мінфіну, Мінюсту України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5/. URL: http://zakon.rada.gov.ua/laws/show/v0114900-12/print