УДК 343.13
DOI https://doi.org/10.32782/2524-0374/2022-10/194

ТЕОРЕТИЧНІ ТА ПРАКСЕОЛОГІЧНІ АСПЕКТИ ФІКСУВАННЯ ТА ВИКОРИСТАННЯ У КРИМІНАЛЬНОМУ ПРОЦЕСУАЛЬНОМУ ДОКАЗУВАННІ ІНФОРМАЦІЇ З ІНТЕРНЕТ-ДЖЕРЕЛ

THEORETICAL AND PRAXEOLOGICAL ASPECTS OF RECORDING AND USING INFORMATION FROM INTERNET SOURCES IN CRIMINAL PROCEDURAL PROOF

Тетерятник Г.К., д.ю.н., професор,
завідувач кафедри кримінального процесу
Одеського державного університету внутрішніх справ

Виходець Ю.О., доктор філософії,
начальник
Департаменту кіберполіції Національної поліції України

Стаття присвячена дослідженню теоретичних та праксеологічних питань фіксування та використання у кримінальному процесуальному доказуванні інформації з Інтернет-джерел.

Авторами зазначається, що цифровізація кримінального провадження як закономірна тенденція його розвитку у сучасному світі, а також соціально-політичні умови: військова агресія російської федерації, тимчасова окупація окремих територій, воєнний стан, значний обсяг кримінальних проваджень щодо воєнних злочинів впливають на необхідність широкого використання інформації з Інтернет-джерел та електронних (цифрових) доказів.

Здійснено огляд наукових джерел та нормативної бази, проектів законів щодо фіксування та використання у доказуванні інформації, отриманої під час огляду Інтернет-ресурсів та електронних документів, електронних (цифрових) доказів. Проаналізовані поняття електронних документів, електронних (цифрових) доказів, процесуальні шляхи фіксування інформації з Інтернет-джерел. Наведені приклади зі слідчої та судової практики.

Констатується, що у чинному КПК України відсутнє поняття електронних (цифрових) доказів, недостатньо розроблений процесуальний порядок їх фіксування, неоднозначною є судова практика щодо оцінки допустимості інформації, яка отримується з Інтернет-джерел.

Зазначається, що інформація з Інтернет-джерел може перевірятися та бути використана під час проведення ідентифікації шляхом пред'явлення для впізнання, пред'явлення для впізнання за фотознімками, судової портретної, лінгвістичної експертизи, експертизи матеріалів і засобів відео-звукозапису та ін.

Звертається увага не необхідності унормування питань, пов'язаних із визначенням такого виду огляду, як огляд Інтернет-джерел, доповнення існуючої системи процесуальних джерел доказів електронними (цифровими) доказами, розробки сучасної концепції доказів.

Ключові слова: інформація, докази, електронні (цифрові) докази, документи, електронні документи, джерело доказів, доказування, Інтернет-джерело, огляд, слідча (розшукова) дія, фіксування, показання, протокол.

The article is devoted to the study of theoretical and praxeological issues of recording and using information from Internet sources in criminal procedural evidence.

The authors note that the digitalization of criminal proceedings as a natural trend of its development in the modern world, as well as socio-political conditions: military aggression of the russian federation, temporary occupation of certain territories, martial law, a significant volume of criminal proceedings regarding war crimes affect the need for wide use of information from Internet sources and electronic (digital) evidence.

A review of scientific sources and regulatory framework, draft laws on recording and use in evidence of information obtained during the inspection of Internet resources and electronic documents, electronic (digital) evidence was carried out. The concepts of electronic documents, electronic (digital) evidence, procedural ways of recording information from Internet sources are analyzed. Examples from investigative and judicial practice are given.

It is noted that the current of Criminal Procedure Code of Ukraine lacks the concept of electronic (digital) evidence, the procedural procedure for recording them is insufficiently developed, and judicial practice regarding the assessment of the admissibility of information obtained from Internet sources is ambiguous.

It is noted that information from Internet sources can be checked and used during identification by means of presentation for identification, presentation for identification by photographs, forensic portrait, linguistic examination, examination of materials and means of video and audio recording, etc.

Attention is drawn to the need to normalize issues related to the definition of this type of review, such as the inspection of Internet sources, supplementing the existing system of procedural sources of evidence with electronic (digital) evidence, and developing a modern concept of evidence.

Key words: information, evidence, electronic (digital) evidence, documents, electronic documents, source of evidence, proof, Internet source, inspection, investigative (search) action, recording, testimony, protocol.

Технічний прогрес є невід'ємною складовою нашого життя. Останніми роками у вітчизняній науці кримінального процесу з'являється все більше досліджень, присвячених цифровізації кримінального провадження, що логічно відповідає тенденціям, умовам та обставинам розвитку нашого суспільства та необхідністю «озброювати», розвивати кримінальне процесуальне законодавство за вимогами часу та нагальними потребами. Як справедливо зазначає А. В. Скрипник: поява нового, «цифрового» аспекту звертає до пошуку шляхів вирішення «…споконвічної проблеми пошуку балансу між дотриманням прав і свобод людини й ефективністю боротьби зі злочинністю, який найбільш яскраво проявляється у сфері кримінальної юстиції» [1, с. 7].

Впливають на таку актуалізацію досліджуваного питання і ті соціально-політичні події, які відбуваються в Україні з 2014 року: збройний конфлікт, який з 24 лютого 2022 року перейшов у масштабну військову агресію російської федерації проти України, тимчасова окупація окремих територій, здійснення кримінального провадження в умовах воєнного стану, необхідність розслідувати значну кількість воєнних злочинів та багато інших.

Питанням використання у доказуванні інформації з Інтернет-джерел, електронних (цифрових) доказів присвячені роботи Н. М. Ахтирської, М. В. Багрія, Н. В. Глинської, І. В. Гловюк, Д. І. Клепки, І. О. Крицької, О. П. Метелева, М. І. Пашковського, А. В. Ратнової, А. В. Скрипника, А. В. Столітнього, Д. М. Цехана та багатьої інших вчених. Водночас низка питань щодо збирання, фіксування, дослідження такої інформації і використання її у кримінальному провадженні досі залишається дискусійною.

Метою статті є отримання наукових результатів у вигляді теоретичних положень та напрацюванні на їх основі практичних рекомендацій щодо фіксування та використання у кримінальному процесуальному доказуванні інформації з Інтернет-джерел.

Окремі слідчі (розшукові) дії, які проводяться в умовах надзвичайних правових режимів та у кримінальних провадженнях щодо кримінальних правопорушень, вчинених на тимчасово окупованих територіях мають свої особливості, пов'язані також відсутністю доступу до таких територій. У вивчених нами 498 кримінальних провадженнях, пов'язаних із тимчасово окупованими територіями, у 83% проводилися огляди різноманітних інтернет-ресурсів [2, с. 297].

Значний обсяг інформації, що має значення для кримінального провадження, отримується із відкритих джерел Всесвітньої комп'ютерної мережі Інтернет. Відповідно до визначення, яке надається у Протоколі Берклі, інформація з відкритих джерел включає загальнодоступну інформацію, яку будь-який представник громадськості може спостерігати, купувати чи запитувати, не вимагаючи особливого правового статусу чи несанкціонованого доступу [3].

Зазначена інформація повинна бути оформлена у процесуальному порядку. Як правило, відомості, отримані слідчим із Інтернету, оформлюються протоколом огляду. Однак, відповідно до ч.1 ст. 237 КПК України передбачає тільки огляд місцевості, приміщення, речей і документів. У чинному КПК України чітко визначена мета проведення кожної слідчої (розшукової) дії. Метою огляду є виявлення та фіксація відомостей щодо обставин вчинення кримінального правопорушення. На це направлений і огляд інформації з Інтернет джерел. Втім, чи можемо ми віднести інформацію з Інтернет сторінки до категорії «документ» або ж «електронний документ». Зазначене питання лежить у площині спірних. Воно звертає нас до проблематики визначення статусу електронних документів у кримінальному провадженні, а також їх використання як джерел доказів.

Відповідно до ч.2 ст. 84, п.2 ч.2 ст. 99 КПК України протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії, складені у встановленому КПК України порядку, відносяться до процесуального джерела доказів – документів. Відповідно до ст. 99 КПК України: «Документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження» [4]. КПК України не дає роз'яснення понять «письмовий» та «електронний» документ, тож для визначення проблемних питань, які пов'язані з цими видами документів, звернемося до нормативної бази.

Згідно зі ст. 1 Закону України «Про інформацію» № 2657-XII від 02.10.1992 року, «документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі» [5]. Відповідно до Національного стандарту України «Діловодство й архівна справа. Терміни та визначення понять» (ДСТУ 2732:2004): п. 3.33 електронний документ – документ, який створюють та використовують тільки в межах комп'ютерної системи [6]. У той же час, ДСТУ 2732:2004 не містить поняття електронного документування та документообігу.

Порядок електронного документообігу визначається Законом України «Про електронні документи та електронний документообіг» №851-IV від 22 травня 2003 року: «Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною» [7]. Відповідно до статті 6 зазначеного закону, створення документу завершується накладенням електронного підпису, за допомогою якого може бути ідентифікований автор документу.

Електронний документ відрізняється від письмового друкованого тим, що інформація у ньому може фіксуватися, хоча і за рахунок письмових символів, але які набувають форми електронних даних. Тобто кожен письмовий символ має відповідне електронне шифрування, завдяки чому такий документ створюється за рахунок відповідної програми, може зберігатися, передаватися, перетворюватися тощо.

Особливістю електронного документа є наявність метаданих, які у кримінальному процесуальному доказуванні відіграють роль одного з критеріїв належності та допустимості такої електронної форми інформації. Метадані забезпечують інформацію про автора, час створення документу, значення даних у момент отримання (спадковість) даних і про подальший шлях від джерела до поточного місця перебування. Вони дають можливість ідентифікувати автора, визначити співвідношення інформації у документі до часу, обставин, які мають значення для кримінального провадження, з'ясувати оригінальність даних в електронному документі [8, с. 119].

У наукових джерелах останнім часом значна увага приділяється питанням процесуального оформлення та використання електронних документів у доказуванні, електронному документообігу у різних сферах життєдіяльності. Концептуально питання електронних, цифрових доказів розглядається у новітніх дисертаційних роботах А. В. Столітнього [9], А. В. Скрипника [10], А. В. Ратнової [11]. Активно декілька десятиліть цифрова криміналістика розвивається у багатьох країнах світу, свідченням чому є різноманітні міжнародні проекти, наукові, методичні розробки, направлені на забезпечення процесу розслідування з використанням цифрових доказів [11, с. 7 – 11; 22 – 24]. У зазначених матеріалах досить детально описуються процедури поводження із різними джерелами електронних доказів, цифровою інформацією, особливостями їх використання у процесі доказування. Натомість у вітчизняному правовому полі існує нормативна прогалина у частині визначення та нормативного закріплення поняття електронних (цифрових) доказів, їх збирання, перевірки та оцінки у кримінальному процесі. Зауважимо, що, на нашу думку, КПК України у цьому питанні відстає від інших процесуальних кодексів, у яких Законом України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» № 2147-VIII від 03.10.2017 року були внесені зміни у частині унормування поняття та порядку використання електронних документів у судочинстві [12].

Слід зазначити, що законодавчі спроби щодо закріплення у КПК України норм, які визначають поняття та порядок використання у доказуванні електронних доказів, були прийняті у Проєкті Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» № 4004 від 01.09.2020 року. У ньому пропонувалося главу 4 «Докази і доказування» розділу I «Загальні положення» доповнити параграфом 4 – 1 «Електронні докази», у якому визначити поняття електронних доказів, порядок їх зберігання, а також визначалися особливості їх збирання шляхом тимчасового доступу до інформації в електронній (цифровій) формі [13]. У Проєкті Закону України «Про внесення змін до Кримінального процесуального кодексу України

та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» №4003 від 01.09.2020 р. У ч. 1 ст. 166-1 зазначеного законопроєкту пропонувалися підстави термінового збереження інформації, у абзаці 2 зазначалося: «Термінове збереження інформації полягає в невідкладному фіксуванні та подальшому зберіганні інформації в електронній (цифровій) формі, яка має значення для встановлення обставин у кримінальному провадженні» [14]. Втім зазначені пропозиції не були підтримані.

Звертаючись до наукових досліджень з цієї проблематики, слід зазначити, що вчені визначають за особливостями роботи із комп'ютерною технікою та відповідним апаратним та програмним забезпеченням, яке використовується для їх огляду, електронні документи можна поділити на: 1) електронні документи на фізичних носіях інформації; 2) електронні документи у вигляді публікацій у мережі Інтернет; 3) електронні документи, розміщені у хмарних сервісах зберігання інформації [11, с.122, 184]. Відповідно до процесуальних вимог отримання електронної інформації, умовно такі процедури можна поділити на: 1) огляд Інтернет-ресурсів, доступ до електронних інформаційних систем або їх частини яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту (гласна слідча (розшукова) дія); 2) огляд в порядку зняття інформації з електронних інформаційних систем (НСРД).

У проаналізованих нами дослідженнях з кримінального процесу науковцями пропонуються визначення електронних (цифрових) доказів та документів [10, с. 10; 11, с. 184; 15, с. 125; 16, с. 258]. Попри зрозуміло відрізнене авторське бачення таких понять, учені спільні у цілісному сприйнятті електронного документу, електронного (цифрового) доказу як інформації (фактичних даних), цифрових даних, які формують такий документ, його носія, необхідності нормативного закріплення понять у КПК України та визначення основних засад та алгоритмів використання таких доказів у кримінальному провадженні.

Як свідчить правозастосовна практика, протоколи огляду Інтернет-ресурсів, доступ до електронних інформаційних систем або їх частини яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, сприймаються судами як докази у кримінальних провадженнях (у цьому підрозділі саме такі електронні документи та докази будуть розглянуті), утім суди аргументують свою позицію у таких випадках здебільшого вказівкою у протоколах огляду на алгоритм отримання такої інформації, наявні додатки до протоколу (стенограму відео-, аудіо- записів, фототаблиці, у т.ч. з використанням скріншотів, записи вилученої інформації на матеріальних носіях), відповідність доступу до Інтернет-ресурсів та порядку вилучення і фіксування інформації з них встановленим законодавством вимогам, а також, як і визначено ст. 94 КПК України, оцінюють кожний доказ з точки зору належності, допустимості, достовірності, а сукупність зібраних доказів - з точки зору достатності та взаємозв'язку для прийняття відповідного процесуального рішення.

Проведення огляду Інтернет ресурсів при розслідуванні кримінальних правопорушень в умовах відсутності доступу до тимчасово окупованих територій та в умовах воєнного стану є досить поширеною слідчою (розшуковою) дією. Водночас відсутність правової регламентації категорій «електронний документ», «електронний доказ», відсутніть у ст. 237 КПК України огляду таких документів, цифрових ресурсів, робить неоднозначним розумінням процесуальної природи таких та вказує на необхідність нормативної регламентації. Наприклад, окремі науковці та практики вказують на те, що в окремих слідчих підрозділах існує практика отримання фактичних даних з мережі Інтернет шляхом проведення НСРД в порядку ч. 2 ст. 264 КПК України. Утім, як справедливо зазначається, така практика створює низку проблем, пов'язаних із засекречуванням відповідних протоколів, їх подальшим розсекречуванням та повідомленням осіб про проведення стосовно них НСРД [17, с. 134]. Фіксування огляду Інтернет-ресурсу протоколом огляду речі – електронно-обчислювальної машини (ЕОМ), під'єднаної до відповідної телекомунікаційної мережі, на нашу думку, теж не зовсім вірно, адже об'єктом огляду виступає не сама ЕОМ, а відповідний цифровий ресурс, який міститься інформацію, що має значення для кримінального провадження. Протокол огляду документу також не відповідає змісту проведення огляду електронних документів, адже останній пов'язаний із подоланням певної логічної інформаційно-технічної схеми доступу, яка має бути детально відображена у протоколі огляду. Якщо документ у розумінні матеріального носія отримується під час проведення інших процесуальних дій (тимчасового доступу до речей і документів, огляду місця події, обшуку тощо), то цифрова інформація може бути отримана, а її змістовна частина вилучена безпосередньо під час огляду Інтернет-ресурсів. При цьому, на відміну від звичайного документа, який має зовнішню форму та зміст, електронний документ містить іще і цифрову складову, яка може змінюватися в іншому порядку, аніж у паперовому документі. Такі цифрові сліди також можуть бути доказами у кримінальному провадженні. Починаючи, від визначення локації у дописі, що може бути використано як факт підтвердження знаходження особи на певній території, так і визначення факту знаходження серверного комп'ютерного обладнання на території іншої держави або тимчасово окупованих територіях [18]. Останні дії, логічно, як правило, пов'язані із доступом до електронних інформаційних систем або їх частини який обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.

Водночас корисною може стати інформація про ідентифікатор підозрюваного (ID), а також наприклад, зображення, які викладаються користувачами, оскільки вони можуть містити метадані з інформацією про дату та час, місце створення та завантаження зображення [19, с. 37]. Так, шляхом нескладних дій при виявлені у пошуковій системі «Google» необхідного зображення можна подивитися властивості певного завантаженого файлу, серед яких є функція «код», в якій міститься інформація про дані файлу (дата завантаження, сайт, на який завантажено, обсяг файлу тощо). У випадку проведення оглядів, у яких необхідні спеціальні знання для розшифровки таких даних доцільно залучення представників підрозділів кіберполіції у якості спеціалістів. Натомість у випадках, коли огляд Інтернет-ресурсів відбувається шляхом сприйняття-відтворення візуалізованої інформації, достатньо навичок слідчого. Відтак, хоча рекомендації багатьох науковців щодо необхідності провадження слідчих (розшукових) дій, що пов'язані з оглядом та вилученням комп'ютерної інформації за участю спеціаліста [20, с. 8], є логічними у випадках вилучення такої інформації під час проведення обшуку, тимчасово доступу до ЕОМ, НСРД, але під час проведення огляду не пов'язаного із доступом до електронних інформаційних систем або їх частини, який обмежується її власником, володільцем або утримувачем або не пов'язаного з подоланням системи логічного захисту, така участь є необов'язковою.

Відтак, необхідним є внесення змін до чинного КПК України: нормативне визначення та закріплення поняття «електронний (цифровий) доказ», доповнення ч. 1 ст. 237 КПК України після слів «речей та документів» формулюванням «електронних документів».

Слід говорити про те, що особливості доказування у кримінальних провадженнях в умовах надзвичайних правових режимів вимагають напрацювання нетрадицій-

них підходів до отримання доказів, водночас такі процедури повинні знайти своє нормативне закріплення. Наведемо приклад із власної слідчої практики. під час допиту свідок, який був присутній під час подій, пов'язаних із окупацією Криму заявив клопотання про те, що він може дати детальний опис подій, але для цього необхідно звернутися до фотознімків та відео, розміщених в мережі Інтернет. Зазначене клопотання було задоволене. Водночас ч.6 ст. 224 КПК України зазначає, що допитувана особа має право використовувати власні документи і нотатки. Процесуально такі дії можна оформити, провівши окремо допит свідка, а потім провести з його участю огляд Інтернет-ресурсів. Водночас, у такому випадку втрачається цілісне сприйняття описуваних подій під час допиту та огляду Інтернет-ресурсу. Інформація зі Всесвітньої мережі не є «власними документами і нотатками», однак такі дії не порушують нічиї права, тож, на мій погляд, є цілком допустимими. Свідок, звернувшись до одного із сайтів, на Google карті показав розташування об'єкту, окремі будівлі, з яких відбувалося захоплення, а також вказав на низку осіб, які брали участь у захопленні стратегічного об'єкту в АР Крим, що було зафіксовано у протоколі допиту, зроблені відповідні скріншоти. Далі свідку було запропоновано ознайомитися зі створеним в ГУНП в АР Крим та м. Севастополі реєстром не передбаченого законами збройного формування так званої «Самооборони Криму». Після чого свідок вказав на низку осіб, яких він бачив під час подій, і які, окрім того, зафіксовані на фото та відео із зазначеного ним сайту, при чому з прив'язкою їх до конкретної дислокації на об'єкті, який було захоплено. По суті, описана слідча (розшукова) дія – допит, вмістила у собі і певні риси огляду, і пред'явлення для впізнання за фотознімками. Тим самим, завдяки одній логічно побудовані комплексній слідчій (розшуковій) дії вдалося отримати важливі фактичні дані, що мають значення для кримінального провадження [21, с. 166 – 169].

Проведення таких гібридних дій, звісно є дискусійним. У ч. 4 ст. 237 КПК України зазначається, що особи, у присутності яких здійснюється огляд, при проведенні цієї слідчої (розшукової) дії мають право робити заяви, що підлягають занесенню до протоколу огляду. Слід підкреслити, що законодавцем інформація, яка надходить від учасника огляду є не показаннями, а саме заявами. Суперечливою є практика ВС у цьому питанні. У постанові Об`єднаної палати ККС ВС від 14.09.2020 у справі № 740/3597/17 було визначено, що: «змістом показань як процесуального джерела доказів **є лише відомості, повідомлені на допиті або одночасному допиті двох чи більше раніше допитаних осіб** *(виділено авторами)*. Термін «показання» в контексті ч. 4 ст. 95 КПК законодавець використовує для позначення відомостей, які надаються в судовому засіданні під час судового провадження. Правило, закріплене в цій нормі, має застосовуватися лише до відомостей, що відповідають ознакам показань як самостійному процесуальному джерелу доказів за вимогами ст. 95 цього Кодексу» [22]. У постанові Об`єднаної палати ККС ВС від 04 лютого 2019 року у справі № 480/100/17 було обґрунтовано більш широке тлумачення терміну «показання»: «…Це правило [частини 4 статті 95 КПК] поширюється на показання, які надаються під час будь-якої слідчої дії, незалежно від класифікації цієї дії органом досудового розслідування. Крім того, у КПК термін «показання» означає не лише твердження, які даються під час допиту особи, що проводиться відповідно до статті 224 КПК, а будь-які твердження особи, надані слідчому, прокурору під час будь-якої слідчої дії» [23]. І хоча цитовані частини постанов стосуються питання безпосередності дослідження показань у суді, вони звертають до проблематики визначення процесуальної природи показань та можливості отримання відомостей щодо відомих учасникам обставин у кримінальному провадженні, що мають значення для цього кримінального провадження, під час інших слідчих (розшукових) дій.

Вчені, які досліджували це питання, прямо чи опосередковано стверджують, що показання можуть отримуватися не тільки під час допитів, сама правова природа показань визначає можливість отримання таких відомостей під час проведення інших слідчих (розшукових) дій [24, с. 3; 8, с. 61]. М.Є. Шумило справедливо зазначає: «…у доказуванні в кримінальній справі реально важливою є не стільки джерельна основа, скільки те, які саме висновки будуть зроблені суб'єктом доказування із отриманого доказового матеріалу» [25, с. 14]. Л.М. Лобойко у своїх роботах досить давно акцентує увагу на тому, що вирішальну роль у провадженні відіграє доказова сила інформації, а не її носій [26, с. 3 – 5]. Відтак, на нашу думку, необхідним є наукове переосмислення існуючої законодавчої концепції доказів, з урахуванням сучасних джерел інформації, їх специфіки та внесення нормативних змін до ст. 84 КПК України.

У чинному КПК України визначена мета кожної слідчої (розшукової) дії, а ч.2 ст. 223 КПК України, що підставами для проведення є достатність відомостей, що вказують на досягнення її мети. Чи є вищенаведений порядок проведення слідчих (розшукових) дій з фіксування інформації з Інтернет-джерел процесуально допустимим – питання дискусійне. Втім, право як регулятор правовідносин, особливо у наш час постійних стрімких змін, повинно швидко адаптуватися, проходячи точку біфуркації, тим самим забезпечуючи належне функціонування правових норм як регуляторів у суспільстві та державі [27, с. 157; 2, с. 297 – 310].

Сьогодні важливим інструментом фіксування інформації з Інтернет-ресурсів – відкритих джерел є Протокол Берклі – практичний посібник з використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, права людини та гуманітарного права, розроблений школою права Університету Каліфорнії в Берклі разом з представниками ООН Протокол Берклі про дослідження цифрових відкритих джерел [3]. У ньому містяться керівні положення щодо міжнародних стандартів для проведення інтернет-розслідувань передбачуваних порушень, керівництво про методи та процедури для збирання, аналізу та зберігання цифрової інформації з дотриманням професійних, правових та етичних принципів. Відповідно до нього з метою правильного збору та збереження отриманих даних і недопущення видалення інформації з мережі Інтернет розроблений відповідний алгоритм, який у тому числі передбачає архівізацію, опис у протоколі огляду процесу отримання та змісту інформації, графічну візуалізацію та вимоги щодо збереження на відповідному носії [3]. Суддя О. Яновська зазначає, що цифрова копія такого документа буде прирівнюватися до оригіналу, має зберігатися у тому вигляді, в якому вона створювалася, що означає збереження оригіналу зібраного цифрового елемента у всіх форматах, в яких він був зібраний [28].

Механізм перевірки та оцінки доказів, отриманих під час огляду Інтернет-ресурсів також має комплексну структуру. Особистість, інформація щодо якої виявлена під час таких оглядів може ідентифікуватися шляхом пред'явлення для впізнання, пред'явлення для впізнання за фотознімками (за відсутності такої особи, що досить поширено у провадженнях в умовах надзвичайних правових режимів та тимчасово окупованих територій); проведенням судової портретної експертизи за експертною спеціальністю 6.2 (ідентифікація особи за ознаками зовнішності за матеріальними зображеннями); проведенням судової експертизи матеріалів і засобів відео-звукозапису (фоноскопічної) експертизи та ін.

Огляд Інтернет-ресурсів надає можливість встановлення не тільки особи підозрюваного (обвинуваченого) та його причетності до кримінального правопорушення,

але й часто є джерелом відомостей про раніше не виявлені та не зареєстровані кримінальне правопорушення. Крім того, у контексті подій, які відбуваються, необхідним є проведення лінгвістичних експертиз (проведення семантичних досліджень усного мовлення, під час вирішуються питання, пов'язані з аналізом змісту мовлення особи (розмови)), що здебільшого проводяться саме за відомостями, отриманими з Інтернет-ресурсів [2, с. 310].

Попри існуючу на сьогодні практику збирання, перевірки, оцінки та використання у доказуванні інформації з Інтернет-ресурсів, відкритих джерел, електронних (цифрових) доказів у кримінальному провадженні питання нормативного вирішення цих питань залишається відкритим. На нашу думку, у КПК України мають бути закріплені норми, які визначаються поняття електронних (цифрових) доказів, механізми їх отримання та використання. Питання процесуального порядку збирання та використання у доказуванні інформації з Інтернет- ресурсів, електронних (цифрових) доказів в цілому вказують, що у сучасній парадигмі увага науковців та законодавця має бути звернена і на більш масштабне питання – розробку нової, сучасної концепції доказів та її втілення у законодавстві.

ЛІТЕРАТУРА

1. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Харків: Право, 2022. 408 с.
2. Тетерятник Г.К. Кримінальне провадження в умовах надзвичайних правових режимів: теоретико-методологічні та праксеологічні основи: монографія. Одеса: Видавничий дім «Гельветика», 2021. 500 с.
3. Berkeley Protocol on Digital Open Source Investigations. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.
4. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI. *Відомості Верховної Ради України*. 2013. № 9-10, № 11-12, № 13. Ст. 88.
5. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
6. Національний стандарт України «Діловодство й архівна справа. Терміни та визначення понять» (ДСТУ 2732:2004). Київ: Держспоживстандарт України. 2005.
7. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. №851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.
8. Давидова Д.В. Джерела доказів у кримінальному процесі України: дис... канд. юрид. наук: 12.00.09. Кривий Ріг, 2015. 209 с.
9. Столітній А.В. Електронне кримінальне провадження на досудовому розслідуванні: дис. … докт. юрид. наук: 12.00.09. Дінпропетровськ, 2018. 648 с.
10. Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні: дис. … канд. юрид. наук: 081-Право. Х., 2021. 379 с.
11. Ратнова А.В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис... канд. юрид. наук: 081 - Право, 2021. Львів. 248 с.
12. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів: Закон України від 03.10.2017 р. № 2147-VIII. URL: https://zakon.rada.gov.ua/laws/show/2147-19#n2.
13. Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів: Проект Закону України № 4004 від 01.09.2020 року. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771.
14. Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам: Проект Закону України №4003 від 01.09.2020 р. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770.
15. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий* вісник Ужгородського національного університету. Серія : Право. 2016. Вип. 36(2). С. 123-125.
16. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий* вісник Міжнародного гуманітарного університету. 2013. № 5. С. 256–259.
17. Просняк А.О., Мигалатій С. О. Особливості досудового розслідування злочинів, вчинених на тимчасово окупованій території України (АР Крим та м. Севастополь). *Досудове розслідування: актуальні проблеми та шляхи їх вирішення:* матеріали постійно діючого наук.-практ. семінару (м. Харків, 26 жовт. 2018 р.) / редкол.: М. В. Членов (голов. ред.), Л. М. Леженіна (заст. голов. ред.), О. В. Косьмін. Харків : Право, 2018. Вип. 10 (ювіл.). С. 132-136.
18. СБУ встановила російське походження останніх хакерських атак на урядові та інфраструктурні інфосистеми. Детектор М. Медіа. URL: https://detector.media/infospace/article/133393/2017-12-30-sbu-vstanovyla-rosiyske-pokhodzhennya-ostannikh-khakerskykh-atak-na-uryadovi-ta-infrastrukturni-infosystemy/.
19. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.
20. Одерій О. В., Корона С. О., Самойлов С. В. Тактика слідчого огляду комп'ютерних систем та їх елементів. Донецьк, 2010. 88 с.
21. Тетерятник Г.К. Гібридизація слідчих (розшукових) дій. *Кримінальне та кримінальне процесуальне законодавство у контексті судової реформи в Україні* (м. Львів, Львівський державний університет внутрішніх справ, 15 червня 2018 р.). Львів: ЛьвДУВС, 2018. С. 166 – 169.
22. Постанова Об`єднаної палати ККС ВС у справі № 740/3597/17 від 14.09.2020р. URL: https://protocol.ua/ru/vs_kks_vidomosti_yaki_nadayutsya/.
23. Постанова Об`єднаної палати ККС ВС у справі № 480/100/17 від 04 лютого 2019 р. URL: https://reyestr.court.gov.ua/Review/87602685.
24. Нарійчук О.Д. Показання обвинуваченого як джерело доказів у кримінальному процесі України: автореф. дис.…канд.. юрид наук : 12.00.09. К., 2012 . 20 с.
25. Шумило М.Є. Гносеологічна і процесуальна природа доказів у Кримінальному процесуальному кодексі України. *Актуальні питання кримінального процесуального законодавства України* (Київ, 26 квітня 2013 року): збірник матеріалів міжвузівської наукової конференції. Національна академія прокуратури України. К.: Алерта, 2013. С.13-27.
26. Лобойко Л.М. Реформування кримінального процесуального законодавства у частині регламентації окремих питань доказування. *Часопис Національного університету «Острозька академія». Серія «Право».* 2011. №2 (4). С.3-5.
27. Тетерятник Г.К. Біфуркація як передумова диференціації процесуальної форми. Оперативно-розшукова діяльність та кримінальний процес: теоретико-праксиологічний дискус щодо їх співвідношення в умовах реформування органів внутрішніх справ України : матеріали Міжнар. наук.-практ. конф. (Одеса, 22-23 квітня 2015 р.). Одеса, 2015. С.157 –159.
28. Яновська О. Докази та доказування у кримінальному провадженні в умовах воєнного стану: практика Верховного Суду. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2022_prezent/2022_09_28_Ianovska_.pdf