СМАЛЬ І. А.,
аспірант кримінального, кримінально-виконавчого права та кримінології
(Академія Державної пенітенціарної служби)

УДК 343.2
DOI https://doi.org/10.32842/2078-3736/2021.4.30

ПРОБЛЕМНІ АСПЕКТИ ЗАСТОСУВАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ СУДОЧИНСТВІ

У статті розглянуто основні проблеми, пов'язані з появою нового виду доказів – електронних доказів. Інтерес до проблеми дедалі більше зростає, оскільки впродовж останніх років науковці порушують питання про необхідність трансформації норм доказового права через широке використанням на практиці нових джерел доказової інформації, які мають цифрову природу.

Проведено аналіз наукових міркувань щодо визначення поняття електронних доказів. На підставі аналізу наукових джерел і судової практики досліджено правову природу електронних доказів у кримінальному судочинстві. Сформулювало авторське бачення поняття електронних доказів і зроблено спробу визначити основні ознаки. Пропонується електронні докази визначити як фактичні дані, які зберігаються чи передаються в електронній (цифровій) формі, отримані в порядку, передбаченому КПК України, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. На підставі аналізу чинного законодавства України, судової практики зроблено висновок про необхідність внесення змін до Кримінального процесуального кодексу України, які стосуються: визначення поняття та видів електронних доказів із доповненням переліку процесуальних джерел доказів. Акцентовано увагу на відсутності чіткої правої процедури надання доступу до інформації, яка міститься на мобільному телефоні та яка забезпечувала б дотримання конституційних прав і законних інтересів особи. Проаналізовано судову практику щодо надання доступу до інформації, яка міститься на мобільному телефоні, та акцентовано увагу на необхідності внесення змін у статтю 264 КПК України. Констатовано важливість і необхідність внесення в КПК України норм, які визначали б проведення обшуку електронного носія інформації як окремої слідчої дії.

Ключові слова: *електронні докази, електронна форма інформації, обшук електронного носія інформації, надання доступу до інформації.*

Smal I. A. Problem aspects of application of electronic evidence in criminal judicial procedure

This article discusses the main problems associated with the emergence of a new type of evidence – electronic evidence. Interest in the problem is growing, as in recent years scholars have been raising the question of the necessity to transform the rules of evidence in connection with the widespread use in practice of new sources of evidence of a digital nature.

An analysis of scientific considerations on the definition of electronic evidence has been made. Based on the analysis of scientific sources and case law, the legal nature of electronic evidence in criminal proceedings has been studied. The author

has formulated her own vision of the concept of electronic evidence and an attempt has been made to determine the main features. It is proposed to define electronic evidence as factual data stored or transmitted in electronic (digital) form, obtained in the manner prescribed by the CPC of Ukraine, on the basis of which the investigator, prosecutor, investigating judge and court establish the presence or absence of facts and circumstances relevant to criminal proceedings and subjected to be proved. Based on the analysis of current legislation of Ukraine and case law it has been concluded that it is necessary to make changes to the Criminal Procedure Code of Ukraine which relate to: the definition of the concept and types of electronic evidence, supplementing the list of procedural sources of evidence.

Emphasis is made on the lack of a clear legal procedure for providing access to information contained on a mobile phone and which would ensure respect for the constitutional rights and legitimate interests of the individual. The court practice on providing access to information contained on a mobile phone has been analyzed and attention is focused on the need to amend Article 264 of the CPC of Ukraine. The author underlines the importance and necessity of introducing norms that would determine the search of electronic media as a separate investigative action into the CPC of Ukraine.

Key words: *electronic evidence, electronic form of information, search of electronic information carrier, granting access to information.*

Вступ. З розвитком цифрових технологій дедалі більшою є доступність персональних цифрових пристроїв та їх різноманіття, а також надзвичайно поширеною є мережа Інтернет, де поступово зникають географічні ознаки злочинності. Зараз необов'язково перебувати в конкретній країні, щоб скоїти кримінальне правопорушення на її території. Відповідно, і виявляти злочинців стало набагато складнішим. З огляду на це останніми роками науковці обговорюють питання розроблення нормативно-правової бази, яка давала б можливість використовувати електронні докази в процесі розслідування злочинів. Електронні докази самі собою можуть виступати також і знаряддям, і засобом скоєння злочинів. Наприклад, розділ XVI Кримінального процесуального кодексу України містить перелік злочинів, які скоюються у сфері використання електронно-обчислюваних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку. Конкретними знаряддями скоєння злочинів у цьому випадку можуть виступати програми-шпигуни, комп'ютерні віруси, програми для несанкціонованого доступу тощо. І для дослідження таких доказів необхідні спеціальні методи та засоби, програми. Водночас є проблема дослідження таких доказів у суді .

Крім того, електронні докази можуть створювати загрозу порушення права людини на захист таємниці особистого життя. Електронні носії інформації зумовлюють існування на ньому великої кількості відомостей особистого характеру, що не мають стосунку до кримінального провадження. Усі ці питання є досить актуальними й потребують ґрунтовного дослідження та врегулювання на законодавчому рівні.

Питання електронних доказів у кримінальному процесі у своїх працях вивчали такі вітчизняні та зарубіжні вчені, як: Н.А. Зігура, В.Б. Вехов, А.Г. Волеводз, Т.Е. Кукарнікова, Ю.Ю. Орлов, С.Й. Гонгало, С.С. Чернявський, В.О. Коновалова, Д.М. Цехан, Д.О. Алексєєва-Процюк, О.М. Бриковська, А.В. Столітній, І.Г. Каланча, В.В. Мурадов, І.О. Крицька, Д. Бродський, М. Ян., О.І. Котляревський, Д.М. Киценко, Н.М. Ахтирська, В.В. Мурадов.

Постановка завдання. Метою статті є дослідження наукових підходів щодо розуміння поняття електронних доказів, обґрунтування необхідності законодавчого закріплення поняття електронних доказів у кримінальному процесуальному законодавстві, вивчення та аналіз судової практики щодо надання доступу до інформації, яка міститься на мобільному телефоні.

Результати дослідження. Стрімкий розвиток інформаційно-комунікаційних технологій можна назвати одним із визначальних факторів розвитку сучасного суспільства. Майже всі сфери суспільного життя управляються за допомогою інформаційних технологій, що, відповідно, вплинуло на інститут доказів і доказування у кримінальному процесі. Такі тенденції вимагають належного нормативного врегулювання питання використання електронних доказів у правозастосовній практиці.

Відповідно до ст. 84 Кримінального процесуального кодексу (далі – КПК України), доказами в кримінальному провадженні є фактичні дані, отримані в передбаченому КПК України порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню [1].

Відповідно, КПК України закріплює поняття процесуальних джерел доказів: показання, речові докази, документи, висновки експертів.

Відповідно до положень КПК України електронні докази належать до документів. Так, у п. 1 ч. 2 ст. 99 КПК України зазначено, що до документів можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (зокрема, електронні) [1].

У науковій сфері є різні підходи до розуміння суті електронних доказів.

Так, з часу появи електронних документів у процесі кримінально-процесуального доказування з'явилися думки щодо необхідності виділення як окремого виду доказів – електронних доказів.

В.Б. Вехов у своїй праці «Електронні докази: проблеми теорії та практики» визначив електронні докази як будь-які дані, представлені в електронній формі, на основі яких слідчий, прокурор, суд у визначеному процесуальним законодавством порядку встановлює наявність чи відсутність обставин, які підлягають доказуванню у кримінальному провадженні [2, с. 48].

Не менш цікавою є думка В.В. Мурадова, який зазначає, що електронні докази – це сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв [3, с. 314].

Слушною є позиція Н.А. Зігури та Г.В. Кудрявцевої, які обґрунтовано доводять про необхідність виділення цифрових доказів в окрему групу та визначають електронні докази як комп'ютерну інформацію, тобто відомості, представлені в електронно-цифровій формі на матеріальному носії, створювані програмними засобами фіксації, обробки та передачі інформації, а також набір команд (програм), призначених для використання в ЕОМ або управління нею [4, с. 47].

Д.М. Цехан використовує термін цифрові докази ("digital evidence"), який набув широкого застосування в наукових джерелах зарубіжних країн. Він уважає, що цифрову інформацію з урахуванням унікальних характеристик не може бути віднесено до жодної чинної класифікаційної групи. Під категорією «цифрового доказу» науковець визначає фактичні дані, які представлено в цифровій формі та зафіксовано на будь-якому типі носія, що стають доступними для сприйняття людиною після обробки ЕОМ та на підставі яких слідчий, прокурор, слідчий суддя і суд встановлює наявність чи відсутність фактів та обставин, які мають значення для кримінального провадження та підлягають доказуванню [5, с. 259].

Д.О. Алєксєєва-Процюк та О.М. Бриськовська вважають, що не потрібно ототожнювати поняття «комп'ютерна інформація» та «електронні докази», які є фактичними даними, що зберігаються в електронному вигляді на будь-яких типах електронних носіїв [6, с. 250], та говорять про необхідність виокремлення електронних доказів як різновиду доказів в окреме джерело доказів [6, с. 252].

Н.М. Ахтирська визначає електронні докази як дані, які підтверджують факти, певну інформацію у формі, яка придатна для обробки за допомогою комп'ютерних систем [7, с. 125].

Проаналізувавши позиції науковців, можна зробити висновки, що електронні докази мають велику кількість властивостей, притаманних традиційним формам доказів, проте вони також мають деякі унікальні характеристики.

Електронні докази зберігаються на відповідному носії (наприклад, комп'ютерах, смартфонах, планшетах, телефонах, принтерах, «розумних» телевізорах (Smart TV) і будь-яких інших пристроях, які мають цифрову пам'ять), зовнішніх запам'ятовуючих пристроях (наприклад, зовнішніх жорстких дисках і USB-флеш-накопичувачах), мережевих компонентах і пристроях (наприклад, маршрутизаторах), серверах і хмарному сховищі даних.

До ознак, які характеризують електронні докази, також належить те, що для можливості їх сприйняття та дослідження необхідні спеціальні програмно-технічні засоби.

Характерними відмінностями електронних доказів є те, що електронну інформацію можна копіювати необмежену кількість разів без втрати характеристик електронних доказів.

Електронні докази дедалі частіше стають одним із основних доказів у процесі розслідування кримінальних правопорушень, що зумовлено тим, що збільшується кількість кримінальних правопорушень, які вчиняються за допомогою мережі Інтернет; власники телефонів зберігають на своїх пристроях цінну інформацію: геолокації, фотографії, відео, листування, що можуть містити цінну для правоохоронних органів доказову інформацію.

Ст. 31 Конституції України кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо [8].

Огляд вмісту електронного носія інформації проводиться не тільки з метою виявлення на ньому збережених файлів, а й з метою фіксації листування, яке міститься в SMS та інших повідомленнях. На нашу думку, є дискусійними питання, пов'язані з оглядом інформації, яка міститься в пам'яті телефонів, планшетів, ноутбуків і т.п. без дозволу суду. Адже під час такого огляду порушуються конституційні права учасників кримінального процесу та інших осіб на таємницю листування, телефонних переговорів, оскільки таємниця спілкування є одним із загальних засад кримінального провадження.

Відповідно до п. 8 ч. 1 ст. 1 Закону «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94, інформаційна система – це організаційно-технічна система, у якій реалізується технологія опрацювання інформації з використанням технічних і програмних засобів. Отже, до інформаційних систем належить комп'ютерна техніка, мобільні телефони, планшети та інші пристрої, які використовуються для опрацювання інформації з використанням програмних засобів [9].

На мобільному телефоні будь-якої особи міститься особисте листування з іншими громадянами в SMS-повідомленнях, соціальних мережах, наприклад у «Ватсап», «Телеграм», «Вайбер» тощо.

Норми кримінального процесуального законодавства України (ч. 2 ст. 264 КПК України) визначають, що не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту [1].

Характерно, що в правозастосовній практиці є непоодинокі факти, коли слідчі звертаються до суду з клопотаннями про дозвіл на проведення огляду мобільного телефона, незважаючи на наявність згоди власника (володільця інформації) на проведення огляду, вважаючи, що без дозволу суду ця слідча дія буде проведена з порушенням конституційних норм.

Так, слідчий суддя Бабушкінського районного суду м. Дніпропетровська (справа № 932/268/20 провадження № 1-кс/932/193/20) ухвалою від 17 січня 2020 р. надав тимчасовий доступ до речей і документів у порядку ст.160 КПК України, а саме – до особистого листування та інших записів особистого характеру, зокрема фотографій, відеозаписів, аудіозаписів, які містилися в мобільному телефоні, вилученому під час обшуку. Зі змісту ухвали вбачається, що підозрюваний на досудовому слідстві давав згоду слідчому на проведення огляду його телефонів [10].

Ухвалою слідчого судді Заводського районного суду м. Миколаєва від 9 червня 2020 р (справа № 487/378/19 провадження № 1-кс/487/3702/20) надано доступ до інформації, яка

міститься на мобільних телефонах підозрюваного, з мотивацією своєї позиції, зокрема, тим, що відповідно до п. 6 ч. 1 ст. 162 КПК України особисте листування особи та інші записи особистого характеру належать до охоронюваної законом таємниці, яка міститься в речах і документах [11].

Побутує практика, коли, отримавши доступ до мобільного телефона шляхом його вилучення на підставі ухвали слідчого судді, слідчі фактично, крім опису зовнішніх ознак телефона, оглядають інформацію та інші особисті дані власника телефона, що містяться а пам'яті пристрою. У процесі огляду підбираються паролі до електронних пристроїв, що можна порівняти з обшуком.

Постає також питання, чи законним буде доступ до носія електронної інформації, яка захищена за допомогою біометричного захисту, якщо слідчі органи мають доступ до відбитків пальців власника телефона, який вони отримали законним шляхом (наприклад, під час проведення дактилоскопії).

Так, ухвалою слідчого судді Саксаганського районного суду м. Кривого Рогу від 19 лютого 2020 р. (справа № 214/2400/19 провадження 1-к/с/214/134/20) надано доступ до мобільного телефона, однією з підстав для надання інформації є посилання на те, що власник мобільного телефона відмовляється надати його в добровільному порядку. Тобто в цьому випадку мобільний телефон перебуває у власника і тільки в разі відмови в наданні доступу до мобільного телефона може бути постановлено ухвалу про дозвіл на проведення обшуку, а за цей час уся інформація, що міститься на мобільному телефоні, може бути знищена власником. Окрім того, зі змісту ухвали вбачається, що надається доступ до мобільного телефона шляхом його вилучення, а не до інформації, яка міститься на мобільному телефоні [12].

Слідчий суддя Хмельницького міськрайонного суду Хмельницької області в ухвалі від 13 січня 2020 р. (справа №686/540/20 провадження 1-кс/686/580/20) надав доступ до мобільного телефона підозрюваного, хоча зі змісту ухвали вбачається, що слідчий фактично просив надати доступ до інформації, яка містить на мобільному телефоні [13].

На нашу думку, проєкт закону України від 31 серпня 2020 року № 4004 «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів», ухвалений у першому читанні, який передбачає, зокрема, нову редакцію ч. 2 ст. 264 КПК України «Пошук, виявлення і фіксація відомостей, що містяться в електронних інформаційних системах або їхніх частинах, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту, є слідчою (розшуковою) дією, яка проводиться на підставі постанови прокурора, слідчого» суперечить ст. 31 КПК України та ч. 2 ст. 14 КПК України та може привести до порушення конституційного права, яке передбачає, що втручання в таємницю спілкування можливе тільки на підставі судового рішення [14].

Верховний Суд у постанові від 9 квітня 2020 р. у справі № 727/6578/17 ухвалив, що зняття інформації з електронних інформаційних систем або їхніх частин можливе без дозволу слідчого судді, якщо доступ до них не обмежується їхнім власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту. Зі змісту ухвали вбачається, що інформація, яка малася в телефоні, була досліджена слідчим шляхом увімкнення телефона та огляду текстових повідомлень [15].

Отже, з правової позиції Верховного Суду, яку викладено в цій постанові, убачається, що огляд змісту мобільного телефона, листування без відповідного рішення суду є законним, якщо такий телефон не захищено паролем.

Водночас ч. 1 ст. 258 Кримінального процесуального кодексу визначає, що ніхто не може зазнавати втручання у приватне спілкування без ухвали слідчого судді. Відповідно до п. 4 ч. 4 ст. 258 КПК втручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники спілкування мають достатні підстави вважати, що воно є приватним. Різновидами такого втручання є зняття інформації з електронних інформаційних систем [1].

Поширеною є практика огляду слідчим мобільних телефонів комп'ютерів, планшетів осіб із втручанням у приватне листування без отримання відповідного дозволу. Зазвичай, вилучивши під час обшуку мобільні телефони, комп'ютерну техніку, слідчий доставляє ці речі в службовий кабінет і розпочинає їх огляд, чим, відповідно, здійснює втручання в приватне спілкування у вигляді листування осіб. Потім він складає протокол огляду, який прокурор використовує як доказ під час досудового розслідування.

Вивчення судової практики свідчить про те, що дослідження інформаційного змісту електронних носіїв інформації відбувається зазвичай шляхом огляду. Однак інформація, яку потрібно дослідити, може бути за межами вільного доступу. Для її пошуку необхідно здійснювати цілеспрямовані пошуки у віртуальному середовищі, що має місце тільки під час проведення обшуку.

На нашу думку, процесуальне законодавство необхідно доповнити нормами, які визначали б можливість проведення обшуку електронного носія інформації як окремої слідчої дії. І такий дозвіл на проведення обшуку повинен бути тільки з дозволу суду.

Висновки. Підсумовуючи викладене, необхідно зазначити про необхідність законодавчого закріплення в кримінальному процесуальному законодавстві поняття електронних доказів, їх класифікації, встановлення чіткого порядку їх вилучення, фіксації, критерії визнання їх недопустимими доказами. На нашу думку, доцільно внести в КПК України окрему главу, яка регулювала б інститут електронних доказів; електронні докази визначити як фактичні дані, які зберігаються чи передаються в електронній (цифровій) формі, отримані в порядку, передбаченому КПК України, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлює наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. У ст. 264 КПК України внести положення, які визначали б, що пошук, виявлення і фіксація відомостей, що містяться в електронних інформаційних системах або їхніх частинах, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту та проводиться тільки з дозволу суду. Крім того, необхідно внести в КПК України норми, які визначали б проведення обшуку електронного носія інформації як окремої слідчої дії.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI . Станом на 21.07.2021. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 21.07.2021).

2. Вехов В.Б. Електронні докази: проблеми теорії та практики. *Правопорядок : історія, теорія і практика*. 2016. № 4 (11). С. 46–50.

3. Мурадов В.В. Електронні докази: криміналістичний аспект використання . *Порівняльно-аналітичне право*. Ужгород, 2013. Вип. № 2–3. С. 313–315.

4. Компьютерная информация как вид доказательств в уголовном процессе России : монография / Н.А.Зигура, А.В. Кудрявцева. Москва : Юрилитинформ, 2011. 176 с.

5. Цехан Д.М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий* вісник Міжнародного гуманітарного університету. Юриспруденція. 2013. Вип. 5. С. 256–260.

6. Алєксєєва-Процюк Д.О., Бриськовська О.М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий* вісник публічного та приватного права. 2018. Вип. 2. С. 247–253.

7. Ахтирська Н.М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету : Право.* 2016. Вип. 36. Т. 2. С. 123–125.

8. Конституція України: станом на 1 січня 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 02.07.2021).

9. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. № 80/94. URL https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 16.07.2021).

10. Ухвала слідчого судді Бабушкінського районного суду м. Дніпропетровська від 17 січня 2020 р. URL: https://reyestr.court.gov.ua/Review/87001237 (дата звернення: 30.06.2021).

11. Ухвала слідчого судді Заводського районного суду м. Миколаєва від 9 червня 2020 р. URL: https://reyestr.court.gov.ua/Review/89698366 (дата звернення: 30.06.2021).

12. Ухвала слідчого судді Саксаганського районного суду м. Кривого Рогу від 19 лютого 2020 р. URL: https://reyestr.court.gov.ua/Review/87716378 (дата звернення: 30.06.2021).

13. Ухвала слідчого судді Хмельницького міськрайонного суду Хмельницької області від 13 січня 2020 р. URL: https://reyestr.court.gov.ua/Review/86978632 (дата звернення: 30.06.2021).

14. Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : проєкт закону України від 31 серпня 2020 р. № 4004 http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=69771 (дата звернення: 02.07.2021).

15. Постанова Верховного Суду від 9 квітня 2020 р. URL: https://reyestr.court.gov.ua/Review/88749345 (дата звернення: 30.06.2021).