ISSN 1995-6134

УДК *343.13-044.245:004.085.74*
DOI: http://doi.org/10.5281/zenodo.3577546

М.І. ДЕМУРА,
асистент кафедри кримінального процесу Національного юридичного університету імені Ярослава Мудрого, кандидат юридичних наук, м. Харків, Україна;
e-mail: tlepova.demura.marina@gmail.com;
ORCID: https://orcid.org/0000-0002-5637-3290

Д.І. КЛЕПКА,
науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України, кандидат юридичних наук, м. Харків, Україна; e-mail: klepka.daria@ukr.net;
ORCID: https://orcid.org/0000-0001-8423-4581

І.О. КРИЦЬКА,
асистент кафедри кримінального процесу Національного юридичного університету імені Ярослава Мудрого, кандидат юридичних наук, м. Харків, Україна;
e-mail: ira24kritskaya@gmail.com;
ORCID: https://orcid.org/0000-0003-3676-4582

ЩОДО ОБМЕЖЕННЯ ПРАВ ОСОБИ ПІД ЧАС ВИЛУЧЕННЯ ЦИФРОВИХ ДЖЕРЕЛ ДОКАЗОВОЇ ІНФОРМАЦІЇ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

M.I. DEMURA,
Assistant, Chair of Criminal Procedure, Yaroslav Mudryi National Law University, Ph.D. in Law, Kharkiv, Ukraine; e-mail: tlepova.demura.marina@gmail.com;
ORCID: https://orcid.org/0000-0002-5637-3290

D.I. KLEPKA,
Research Assistant, Research Department of the Criminal Procedure and Judiciary Issues, Academician Stachis Scientific Research Institute for the Study of Crime Problems, National Academy of Legal Sciences of Ukraine, Ph.D. in Law, Kharkiv, Ukraine; e-mail: klepka.daria@ukr.net;
ORCID: https://orcid.org/0000-0001-8423-4581

I.O. KRYTSKA,
Assistant, Chair of Criminal Procedure, Yaroslav Mudryi National Law University, Ph.D. in Law, Kharkiv, Ukraine; e-mail: ira24kritskaya@gmail.com;
ORCID: https://orcid.org/0000-0003-3676-4582

RESTRICTION OF PERSONAL RIGHTS WHEN REMOVING DIGITAL SOURCES OF EVIDENCE IN CRIMINAL PROCEEDINGS

АНОТАЦІЇ (ABSTRACTS), КЛЮЧОВІ СЛОВА (KEY WORDS)

Постановка проблеми. Використання електронної інформації досі залишається майже неврегульованим у національному кримінальному процесуальному законодавстві. Це стосується забезпечення використання цього різновиду інформації та її носіїв у доказуванні у кримінальному процесі та недопущення протиправних і необґрунтованих порушень чи обмежень прав людини (на приватне життя, таємницю листування, власність, підприємницьку діяльність тощо) та її законних інтересів у випадках, коли такі носії інформації мають бути вилучені для виконання завдань кримінального провадження. Тому провідне значення має побудова такого механізму обмеження прав особи під час одержання цифрових носіїв доказової інформації, який би дозволив віднайти необхідний баланс між можливістю здійснення ефективного досудового розслідування та притягнення винних осіб до кримінальної відповідальності з одного боку, й інтересами осіб, яким може бути завдана істотна шкода під час застосування заходів забезпечення

© Демура М.І., Клепка Д.І., Крицька І.О., 2020
Open access under CC BY license

ISSN 1995-6134

кримінального провадження щодо належного їм майна, з іншого боку. **Метою** статті є розкриття правової природи цифрових джерел доказової інформації та їх місця у системі доказів з погляду de jure і de lege ferenda, а також, з'ясування допустимого співвідношення між обмеженням прав особи під час вилучення цифрових доказів та необхідністю формування доказової інформації під час досудового розслідування (на прикладі проекту закону № 9484). **Методи** дослідження обрані з урахуванням специфіки цілей, задач, об'єкта і предмета дослідження. Серед них діалектичний метод, який надав змогу розкрити окремі аспекти обмеження прав особи під час вилучення цифрових джерел доказової інформації у кримінальному провадженні; формально-юридичний (юридико-технічний) метод, що був використаний для вивчення норм права, дослідження особливостей юридичної техніки; герменевтичний, за яким з'ясовано правовий зміст норм КПК та законодавчих пропозицій та виявлені дефекти нормативного регулювання. **Результати.** Зроблений аналіз законодавчих пропозицій, спрямованих на врегулювання окремих аспектів обмеження прав свободи під час вилучення цифрових джерел доказової інформації (на прикладі законопроекту № 9484), дозволив визначити їх недоліки: спроби "вписати" електронні докази у вже існуючу декілька десятиліть систему процесуальних джерел доказів без врахування їх специфічної правової природи; залишення поза увагою випадків, під час яких вилучення цифрових пристроїв об'єктивно необхідно (як, наприклад, проведення експертизи у лабораторних умовах), інакше існує ризик втрати доказової інформації, тощо, а також переваги: намагання визначити місце електронних доказів у системі процесуальних джерел; прагнення віднайти рівновагу між необхідним для виконання завдань кримінального провадження вилученням цифрових носіїв інформації та необґрунтованим обмеженням права власності особи тощо. **Висновки.** Запропоновано розширити перелік процесуальних джерел доказів шляхом доповнення цифровими джерелами доказової інформації.

Ключові слова: *цифрове джерело інформації; обмеження прав особи; доступ та вилучення*

***

Problem statement. The all-embracing technology of social middleware called to penetrate IT to the realms of life. The loss of the electronic information is even lower than that of the national criminal procedural legislation. It is intended to put in order the days, from one side, the question of ensuring that this type of information and its media is used in criminal proceedings and, on the other, to prevent unlawful and unjustified violations or restrictions on human rights (privacy, correspondence, property, business, etc.) and its legitimate interests in cases, when such media should be removed for criminal prosecution purposes. Therefore, the leading role in this respect is to establish such a mechanism for restricting the rights of individuals in obtaining digital media of evidence that would strike the necessary balance between the possibility of an effective pre-trial investigation and the prosecution of perpetrators on the one hand, and the interests of persons who may be materially prejudiced by the enforcement of criminal proceedings against their property, on the other hand. **Purpose:** The articles are to disclose the legal nature of digital sources of evidence and their place in the evidence system from the point of view of de jure and de lege ferenda, as well as to clarify the permissible relationship between the restriction of a person's rights in the seizure of digital evidence and the need to produce evidence during pre-trial investigation (on the example of draft law No. 9484). **Methods** are chosen based on the specifics of the goals, objectives object and subject of the study. The system used the methods of scientific cognition; in particular, the methodological basis was the dialectical method, which allowed revealing certain aspects of the restriction of the rights of the individual while seizing digital sources of evidence in criminal proceedings. In addition, the formal-legal (legal-technical) method was used to study the rules of law, to analyze the features of legal technology; and the hermeneutical method revealed the legal content of the CCP norms, legislative proposals and defects in legal regulation. **Results:** analysis of legislative proposals aimed at regulating certain aspects of the restriction of liberties while retrieving digital sources of evidentiary information (on the example of Bill No. 9484) made it possible to identify their shortcomings: attempts to "incorporate" electronic evidence into an existing system of procedural sources for several decades without regard to their specific legal nature; the neglect of cases where the removal of digital devices is objectively necessary (such as, for example, examination in the laboratory), otherwise there is a risk of loss of evidentiary information, etc., as well as the advantages of: trying to determine the place of electronic evidence in the system of procedural sources; the desire to strike a balance between what is necessary to carry out the criminal proceedings by seizing digital media and the unjustified restriction of the property right of the individual and the like. **Conclusions:** the conducted research gives grounds to argue for the need to expand the list of procedural sources of evidence by supplementing digital sources of evidence.

Key words: *digital source information; restrictions on individual rights; access and deletion*

Постановка проблеми

Поступова всеохоплююча технологізація соціального середовища призвела до проникнення IT до різних сфер життя. Водночас використання електронної інформації досі залишається майже неврегульованим у національному кримінальному процесуальному законодавстві. Зазначене ставить на порядок денний, з одного

ISSN 1995-6134

боку, питання про забезпечення використання цього різновиду інформації та її носіїв у доказуванні у кримінальному процесі, а з іншого – недопущення протиправних і необґрунтованих порушень чи обмежень прав людини (на приватне життя, таємницю листування, власність, підприємницьку діяльність тощо) та її законних інтересів у випадках, коли такі носії інформації мають бути вилучені для виконання завдань кримінального провадження. Тому провідне значення у цьому аспекті має побудова такого механізму обмеження прав особи під час одержання цифрових носіїв доказової інформації, який би дозволив віднайти необхідний баланс між можливістю здійснення ефективного досудового розслідування та притягнення винних осіб до кримінальної відповідальності з одного боку, й інтересами осіб, яким може бути завдана істотна шкода під час застосування заходів забезпечення кримінального провадження щодо належного їм майна, з іншого боку.

Важливим є наукове обґрунтування означеної проблематики, щодо чого, наприклад, О.Г. Григор'єв звертає увагу на кримінальне процесуальне значення комп'ютерної інформації та її місце в теорії доказів, а також межі прикладного використання цього виду інформації у кримінальному процесі; М. А. Іванов характеризує цифрову інформацію та машинні носії у різних формах, встановлює співвідношення між цими об'єктами та речовими доказами і документами, здійснює кримінально-процесуальну класифікацію цифрової інформації та машинних носіїв. С.І. Кувичкова досліджує особливості поділу такої інформації на ту, що характеризується процесуальною природою, та таку, що має "альтерпроцесуальне" походження; Р.І. Оконенк визначає поняття електронних доказів та розкриває їх специфічні властивості, пропонує дефініцію поняття "дослідження електронного доказу" та аналізує можливі форми реалізації цієї діяльності, окреслює напрямки можливого вдосконалення кримінального процесуального законодавства у сфері захисту таємниці приватного життя особи, у контексті вилучення та дослідження електронних носіїв інформації, з урахуванням досвіду США тощо; Д.М. Цехана, вводячи поняття цифрових доказів, надає їх визначення та висвітлює особливості останніх, а також під іншим кутом пропонує поглянути на питання забезпечення дотримання вимог щодо допустимості цих доказів; та багатьох інших.

Слід також звернути увагу на дослідження Ш. Гудісона (Sean E. Goodison, 2015), Р. Девіса (Robert C. Davis, 2015) та Б. Джексона (Brian A. Jackson, 2015), які, оцінюючи переваги використання різноманітних видів цифрової інформації (на кшталт, даних GPS для встановлення перебування підозрюваних на місці злочину або поблизу нього, аналіз текстових повідомлень та електронної пошти, фотографій та метаданих із соціальних мереж) для забезпечення ефективнішого розслідування, звертають увагу на криміналістичні проблеми у використанні цього виду доказів, пропонуючи прикладні напрямки їх вирішення [1]; О. Керр (Orin S. Kerr, 2005), яким проведено аналіз можливості використання класичної моделі кримінального процесуального для врегулювання розслідування, пов'язаного з цифровими доказами, за результатами якого зроблено висновок про необхідність запровадження нових методів збору цифрових доказів, а отже і нових правових стандартів роботи з ними тощо [2]; Ф. Моліна (Fernando Molina, 2017), Г.Д. Родригез, (Glen Dario Rodriguez, 2017), що акцентують увагу на збереженні цифрових доказів у матеріалах кримінальної справи, оцінюючи потенційні ризики втрати важливої доказової інформації [3] тощо.

При цьому, з'ясування юридичної природи цифрових доказів (зокрема, визначення її характерних властивостей та місця з-поміж інших засобів доказування), використання, зберігання такого різновиду доказової інформації, неодмінно пов'язане з обмеженням прав особи у разі вилучення цифрових джерел, як з боку законодавця, підтвердженням чого є різноманітні законопроекти (наприклад, реєстр. № 9484 від 17.01.2019 р., № 2740 від 15.01.2020 р. та ін.), так і з боку правозастовників та зацікавлених у цьому осіб.

Тому метою статті є встановлення правової природи та місця цифрових джерел доказової інформації у кримінальному процесі, виявлення недоліків вітчизняного законодавства та правозастосовної практики стосовно питання їх вилучення, та формулювання пропозицій, спрямованих на подолання цих недоліків. Її новизна полягає в аналізі специфіки вилучення таких об'єктів у кримінальному провадженні, обумовленій необхідністю одночасного врахування як інтересів ефективного досудового розслідування та правосуддя, так і прав приватних осіб; оцінці ризиків, "прихованих" у таких законодавчих ініціативах; та пропозиції способів їх уникнення. Завданням роботи є розкриття правової природи цифрових джерел доказової інформації та їх місця у системі доказів з погляду de jure

ISSN 1995-6134

і de lege ferenda, а також, з'ясування допустимого співвідношення між обмеженням прав особи під час вилучення цифрових доказів та необхідністю формування доказової інформації під час досудового розслідування (на прикладі проекту закону № 9484).

Правова природа та місце цифрових джерел доказової інформації у системі доказів з погляду de jure і de lege ferenda

Щодо встановлення юридичної природи цифрових джерел доказової інформації та визначення їх місця серед процесуальних джерел доказів слід звернути увагу, що у перелічених раніше проектах законів були зроблені спроби вирішити ці завдання, зокрема, шляхом віднесення електронної інформації та її носіїв до речових доказів, за умови відповідності критеріям, передбаченим у ч.1 ст.98 КПК. Попри позитивне прагнення вирішити законодавчі прогалини, подібний підхід до розв'язання цієї прикладної та наукової проблеми, на наш погляд, викликає певні зауваження.

Зокрема, у науковій літературі існує плюралізм думок із цього напрямку, а їх системний аналіз дає підстави для виокремлення принаймні таких чотирьох підходів:

(1) можливість віднесення цієї категорії об'єктів до документів. Зокрема, С.В. Васильєв та Л.М. Ніколенко щодо відео-, аудіозаписів і кіноматеріалів заперечують необхідність виділення їх як самостійного процесуального джерела, акцентуючи при цьому на тому, що саме має першочергове доказове значення у носії – інформація, зафіксована на ньому, а не його фізичні властивості. Водночас вказане обумовлює необхідність перекодування такої інформації із застосуванням спеціальних технічних засобів доказів для ознайомлення з нею під час судового розгляду [4, с.113];

(2) можливість віднесення цієї категорії об'єктів до речових доказів. Так, наприклад, А.С. Білоусов розглядає комп'ютерні об'єкти як один з різновидів окремої групи речових доказів, пояснюючи особливою сферою використання, а саме з метою створення, обробки, накопичення чи передачі інформації в її електронному вигляді [5, с.14];

(3) можливість віднесення цієї категорії об'єктів як до документів, так і до речових доказів. Такого висновку, наприклад, доходить О.Г. Григор'єв [6, с.98], а також М.М. Єгоров, вказуючи на те, що цифрові докази можуть бути визнані як речовими доказами, так і документами, за умови віддання переваги першим за наявності певних спорів або сумнівів при вирішенні цього питання [7, с.19]. Близькою є й позиція С.І. Кувичкова, на думку якого електронна інформація у різних її формах і видах виступає речовим доказом; водночас інформація, представлена в електронному вигляді, буде вважатися таким джерелом доказів як документ, якщо вона зафіксована на будь-якому матеріальному об'єкті з реквізитами, що дозволяють ідентифікувати її та встановити на її основі обставини, які підлягають доказуванню у справі [8, с.15]. Р.І. Оконенко також відстоює подібний підхід, зазначаючи, що при вирішенні питання, в якості чого виступає електронна інформації, доцільно зміст файлу логічно розділити на два види відомостей: основний зміст файлу (відомості, для використання яких файл і був створений) та інформацію про властивості й характеристики файлу (місце знаходження файлу на диску, час створення, внесення змін і т.п.) – якщо значення для провадження, поряд з основним змістом файлу, матиме інформація про властивості файлу, то електронний носій інформації можна розглядати в якості речового доказу, якщо ж значення для справи має лише зміст файлу, то відповідний матеріальний носій може бути залучений до справи в вигляді іншого документа [9, с.17];

(4) *необхідність виокремлення цифрових джерел доказової інформації як самостійного процесуального джерела.* Зокрема, як вказує Д.М. Цехан, це обумовлюється унікальними характеристиками цифрової інформації та її носіїв, насамперед її нематеріальністю [10, с.259]. Керуючись критеріями доказового значення, механізму утворення, сприйняття та середовища існування, Н.А. Зігура та Г. В. Кудрявцева пропонують відмежувати комп'ютерну інформацію від речових доказів [11, с.47]. Не може бути віднесена ані до документів, ані до речових доказів цифрова інформація, зафіксована на машинному носії, і на думку М.А. Іванова, який пропонує виокремити її як самостійне джерело відомостей, керуючись такими специфічними властивостями: (1) неречова природа; (2) природно-технічні особливості створення, обробки, збереження, передачі; (3) особливі кримінальні процесуальні процедури та криміналістичні прийоми її пошуку та вилучення, дослідження, перекодування тощо [12, с.170]. О.П. Метелев, розглядаючи гносеологічну та правову природу цифрових доказів, констатує гіпотетичну можливість віднесення останніх і до речових доказів, і до документів, але при цьому більш логічним

ISSN 1995-6134

також вважає виділення цифрової (електронної інформації як окремого виду доказів у кримінальному процесі [13, с.83].

Підтримуючи аргументацію прихильників четвертого підходу, виокремимо характерні властивості цифрових джерел доказової інформації, що обґрунтовують її особливу процесуальну природу: а) обумовлений відсутністю констатного зв'язку з матеріальним носієм неречовий характер, – зважаючи на це електронна інформація є трансльованою (тобто, може бути переданою з одного носія на інший) та мультиплікативною (одночасного може існувати на різних носіях); б) обов'язковість інтерпретації та перекодування цифрової інформації з використанням спеціальних технічних засобів і програмного забезпечення через неможливість її безпосереднього сприйняття та подальшого дослідження, що обумовлює специфічний порядок збирання, перевірки й оцінки; в) її мінливість, яка проявляється в існуванні можливості дистанційного внесення змін до електронної інформації та її знищення [14, с.102–103].

Отже, *de lege ferenda* (з погляду закону, прийняття якого бажане), уявляється більш вдалим підхід, спрямований на виділення цифрових джерел доказової інформації в якості самостійного процесуального джерела, як, наприклад, зроблено в Кримінальному процесуальному законі Латвії (ст.136 із назвою "Електронні докази", під якими розуміються відомості про факти в формі електронної інформації, обробленої, збережуваної або переданої пристроями або системами автоматизованої обробки даних) [15]. У КПК Молдови частина 9 глави III розділу IV носить назву "Матеріальні засоби доказування", серед яких, зокрема, виділяються й аудіо- та відеозаписи, фотографії та інші носії інформації (ст.164) [16].

У вітчизняному адміністративному, господарському та цивільному процесуальному законодавстві також обрано підхід щодо виділення електронних доказів як самостійного виду доказів (ст.99 КАС, ст.96 ГПК, ст.100 ЦПК). У цьому контексті слід додати, що на думку, наприклад, А.В. Ратнової, попри те, що вказані законодавчі акти і не зачіпають безпосередньо кримінальний процес, такий законодавчий підхід (а саме виділення електронних доказів поряд із речовими та письмовими) є прогресивним і позитивним прикладом і для цієї процесуальної галузі права [17, с.237]. Підтримує таку ідею й А.В. Коваленко, вказуючи, що такого роду законодавчі новели "не мають оминути і кримінальний процес", оскільки "теорія процесуального доказування є міждисциплінарним напрямом наукового пошуку та інтегрованою сферою знань" [18, с.239]. Наведені аргументи близькі й нам, а тому висловлюємо свої сподівання на найскоріше запровадження подібних нормативних приписів і у КПК.

Обмеження прав особи під час вилучення цифрових доказів VS втрата доказової інформації (на прикладі проекту закону № 9484)

Даючи наукову оцінку окремим пропозиціям, зокрема, законопроекту № 9484, слід звернути увагу, що викликає певні застереження ідея доповнити пункт 4 частини шостої статті 100 КПК України новими абзацами четвертим, п'ятим і шостим. Зокрема, цими положеннями передбачається покладення обов'язку "повернення власнику (законному володільцю) або передачі йому на відповідальне зберігання речових доказів, що не містять слідів кримінального правопорушення, у вигляді пристроїв для обробки, передавання та зберігання електронної інформації або їх складових, якщо вони використовуються як предмети або засоби праці та/або вилучення яких може завдати істотної шкоди їх власнику (законному володільцю)" [19]. Тут слід звернути увагу, що повернення речових доказів власнику (законному володільцю) зумовлює поновлення у нього відповідних правомочностей, які випливають з належного йому права власності, у зв'язку з чим виступає одним із способів вирішення долі речових доказів. Таким чином, повернення означає, що матеріальний об'єкт переходить у повне користування та розпорядження відповідної особи з правом його відчуження або, навіть, знищення. Зрозуміло, що такі дії стосовно речових доказів не можуть бути вчинені, оскільки у такому разі не буде забезпечено дотримання засади безпосередності дослідження показань, речей та документів під час судового розгляду.

Виходячи з цього, єдиною підставою для залишення речових доказів, "що не містять слідів кримінального правопорушення, у вигляді пристроїв для обробки, передавання та зберігання електронної інформації або їх складових" [19], у володінні особи, яка їх вилучила, є гіпотетична можливість заподіяння шкоди кримінальному провадженню, якщо зазначений пристрій не буде вилучено. Однак така можливість на вимогу власника (законного володільця) повинна бути письмово обґрунтована в протоколі огляду. Тут слід звернути увагу, що протокол є формою *фіксування* кримінального провадження, а тому

ISSN 1995-6134

його складання спрямоване на закріплення та засвідчення ходу та результатів процесуальних дій. Подібний "технічний" характер цього різновиду процесуальних документів, як уявляється, не передбачає викладення певного обґрунтування або мотивування, оскільки це скоріше властиво процесуальному рішенню.

Уточнення, на нашу думку, потребує й формулювання запропонованого у зазначеному вище законопроекті абз.6 п.4 ч.6 ст.100 КПК України, оскільки залишається не зрозумілим, що є підставою для притягнення особи, яка вилучила зазначені речові докази, до відповідальності – сам факт необґрунтованого вилучення або ж настання негативних наслідків у вигляді знищення чи пошкодження пристроїв через їх необґрунтоване вилучення.

Важливим також є питання про можливі нормативні корективи чинного кримінального процесуального законодавства у контексті застосування окремих заходів забезпечення кримінального провадження щодо цифрових джерел доказової інформації, зокрема, тимчасового доступу до речей і документів, тимчасового вилучення та арешту майна. Наприклад, у п.10-11 законопроекту № 9484 запропоновано внести зміни до ч.2 ст.159 КПК України, шляхом уточнення в дужках словосполучення "у тому числі до пристроїв для обробки, передавання та зберігання електронної інформації або їх складових". Однак, на наш погляд, подібне уточнення носить скоріше вузько спрямований, "точковий" характер. Внесення таких змін не несе жодного нормативного змісту, оскільки вказані правові приписи і так є очевидними. У світлі зазначеного, звертаємо увагу на аналогічне зауваження, яке стосується змін, запропонованих авторами законопроекту до ч.7 ст.163 КПК України.

Аналіз проекту закону № 9484 також засвідчує існування інших, досить суперечливих положень. Йдеться, наприклад, про нову редакцію частини 3, якою пропонується доповнити ст.167 КПК України. Зазначеним нормативним приписом передбачається закріпити заборону "вилучати пристрої для обробки, передавання та зберігання електронної інформації або їх складових, а також порушувати роботу комп'ютерних та інших мереж, якщо знаряддям, засобом або предметом кримінального правопорушення виступає інформація, що в них міститься" [19]. Однак видається доцільним, так само як у частині 4, якою запропоновано доповнити ст.98 КПК України, вказати на можливі винятки із такої заборони, а саме – коли копіювання електронної інформації може спричинити пошкодження чи знищення її самої або пристрою для її обробки, передавання та зберігання.

Розробниками законопроектів зроблені також спроби обмежити можливість накладення арешту на майно, якщо ним є цифрові носії інформації, однак поряд із очевидним позитивом, на нашу думку, подібні пропозиції несуть і потенційні ризики. Так, наразі у чинній редакції ч.2 ст.168 КПК України, забороняється тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом із інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження. Водночас у проекті закону № 9484 передбачається суттєве обмеження наведеної можливості, яка, безумовно, має важливе значення для збирання та перевірки доказів у кримінальному провадженні. Зокрема, системний аналіз запропонованих змін ч.4 ст.98, ч.3 ст.167, ч.2 ст.168, свідчить, що вилученими можуть бути лише ті пристрої для обробки, передавання та зберігання електронної інформації які самі по собі були знаряддям, засобом або предметом кримінального правопорушення. Якщо ж доказове значення має лише електронна інформація, що в них міститься, вона повинна бути скопійована "на місці", без вилучення, навіть тимчасового, її матеріальних носіїв. Уявляється, що вказаний підхід залишає поза увагою ситуації, коли віднайти та відтворити електронну інформацію, що може мати значення для встановлення обставин кримінального провадження, яка зберігалася на пристроях, але була знищена, на місці просто неможливо. Здійснення відповідних дій вимагає проведення комп'ютерно-технічної експертизи стаціонарно із застосуванням спеціальних криміналістичних методів дослідження та спеціального програмного забезпечення.

Контекстно відзначимо, що, як неодноразово вказував у своїх правових позиціях Європейський суд з прав людини (наприклад, у п.150 рішення у справі "Матанович проти Хорватії" від 04.04.2017 р.), "…будь-які труднощі, які виникають у захисту через обмеження права, повинні бути достатньо врівноважені процедурами, які виконують судові органи" [20]. Видається, що забезпечення дотримання розумного балансу публічних і приватних інтересів у наведеній ситуації буде можливим завдяки судовому контролю на етапах вирішення питання слідчим суддею про арешт майна та надання доручен-

Forum Prava, 2020. 60(1). 37–46
(Research Article)

ISSN 1995-6134

ня на залучення експерта та проведення експертизи.

Окремо звернемо увагу на дискусійну пропозицію щодо доповнення ч.5 ст.170 КПК України новим абзацом другим, згідно з яким "арешт на майно у вигляді пристроїв для обробки, передавання та зберігання електронної інформації або їх складових, якщо вони використовуються їх власником (або законним володільцем) як предмети або засоби праці або якщо їх арешт може завдати шкоди фізичній чи юридичній особі, яка не є учасником цього кримінального провадження" [19] дозволяється накладати лише за наявності однієї із таких цілей: 1) забезпечення спеціальної конфіскації; 2) забезпечення конфіскації майна як виду покарання або заходу кримінально-правового характеру щодо юридичної особи.

На практиці поширеним є підхід, викликаний помилковим ототожненням накладення арешту на певні матеріальні об'єкти та вилучення таких об'єктів із фактичного володіння особи. Водночас, відповідно до ч.1 ст.170 КПК, "арештом майна є тимчасове, до скасування у встановленому цим Кодексом порядку, позбавлення за ухвалою слідчого судді або суду права на *відчуження, розпорядження та/або користування* майном…", тобто взагалі не йдеться про позбавлення особи такої правомочності, як *фактичне володіння*. А тому накладення арешту на пристрої для обробки, передавання та зберігання електронної інформації, особливо враховуючи запропоновані у законопроекті № 9484 зміни до ч.12 ст.170, зовсім не значитиме їх вилучення і позбавлення особи можливості використовувати їх як предмети або засоби праці, а лише буде спрямованим на недопущення їх пошкодження, знищення, відчуження іншим особам тощо. Отже, видається доцільним розрізняти наявність підстав для арешту майна та можливість передачі такого майна на відповідальне зберігання власнику. Тому у вказаних ситуаціях може бути запропонований такий алгоритм дій: за наявності підстав, передбачених у ст.170 КПК України, на вказані пристрої може бути накладений арешт, але лише з обмеженням права на розпорядження ними; пристрій або його складові передається власнику (або законному володільцю) на відповідальне зберігання, при цьому у рішенні про передачу мають бути вказані обов'язки особи щодо зберігання такого матеріального об'єкта, а саме: а) зберігати речові докази у належному стані, придатному для використання у кримінальному провадженні; б) заборона відчужувати їх, передавати іншим особам; в) надавати речові докази слідчому, прокурору, суду для проведення необхідних процесуальних дій за першою вимогою.

Висновки

1. Зважаючи на специфічні властивості цифрових джерел доказової інформації, "з погляду закону, прийняття якого бажане", уявляється більш вдалим підхід, який полягає у розширенні переліку передбаченої у ст.84 КПК системи процесуальних джерел доказів шляхом її доповнення цифровими джерелами доказової інформації

2. Зроблений на прикладі законопроекту № 9484 аналіз законодавчих пропозицій, спрямованих на врегулювання окремих аспектів обмеження прав свободи під час вилучення цифрових джерел доказової інформації, дозволив визначити їх недоліки (спроби "вписати" електронні докази у вже існуючу декілька десятиліть систему процесуальних джерел доказів без врахування їх специфічної правової природи; залишення поза увагою випадків, під час яких вилучення цифрових пристроїв об'єктивно необхідно (як, наприклад, проведення експертизи у лабораторних умовах), інакше існує ризик втрати доказової інформації, тощо) переваги (намагання визначити місце електронних доказів у системі процесуальних джерел; прагнення віднайти рівновагу між необхідним для виконання завдань кримінального провадження вилученням цифрових носіїв інформації та необґрунтованим обмеженням права власності особи та ін.) з погляду знаходження розумного балансу між можливістю здійснення ефективного досудового розслідування і притягнення винних осіб до кримінальної відповідальності з одного боку, та інтересами осіб, яким може бути завдана істотна шкода під час застосування заходів забезпечення кримінального провадження щодо належного їм майна, з іншого.

Конфлікт інтересів

Автори статі повідомляють про відсутність конфлікту інтересів.

Вираз вдячності

Дослідження не отримало будь-якої фінансової підтримки з боку юридичних чи фізичних осіб.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sean E. Goodison, Robert C. Davis, and Brian A. Jackson. Digital Evidence and the.U.S. Criminal Justice Sys-

tem. Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. URL: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf&ved=2ahUKEwjohpby6tDnAhVFpYsKHW3wB2cQFjAOegQICBAB&usg=AOvVaw1vdoqPLquJerLLqRJLPd-E&cshid=1581676870679.
2. Orin S. Kerr Digital Evidence and the New Criminal Procedure. *Columbia Law Review.* Vol. 105, No. 1 (Jan., 2005), pp. 279–318 URL: https://www.jstor.org/stable/4099310.
3. Glen Dario Rodriguez, Fernando Molina The preservation of digital evidence and its admissibility in the court. DOI: 10.1504/IJESDF.2017.10002624.
4. Васильєв С. В., Ніколенко Л. М. Доказування та докази у господарському процесі України: монографія. Харків: Еспада, 2004. 192 с.
5. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів: автореф. дис. … канд. юрид. наук: 12.00.09. Київ, 2008. 18 с.
6. Григорьев О. Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: дисс. … канд. юрид. наук: 12.00.09. Омск, 2003. 221 с.
7. Егоров Н. Н. Вещественные доказательства: уголовно-процессуальный и криминалистический аспекты. Москва: Юрлитинформ, 2007. 304 с.
8. Кувычков С. И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: дисс. … канд. юрид. наук: 12.00.09. Нижний Новгород, 2016. 273 с.
9. Окоменко Р. И. Электронные доказательства и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации**:** дисс. … канд. юрид. наук: 12.00.09. Москва, 2016. 158 с.
10. Цехан Д. М. Цифрові докази: поняття, особливості та місце в системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2013. № 5. С. 256–260.
11. Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательств в уголовном процессе России: монография. Москва: Юрлитинформ, 2011. 176 с.
12. Иванов Н. А. Доказательства и источники сведений в уголовном процессе: проблемы теории и практики: монография. Москва: Юрлитинформ, 2015. 232 с.
13. Метелев О. П. Гносеологічна та правова природа цифрових доказів у кримінальному процесі. *Правова позиція*. 2018. № 1(20). С. 75–86.
14. Крицька І. О. Речові докази у кримінальному провадженні: монографія /за наук. ред. А. Р. Туманянц. Харків: Право, 2018. 280 с.
15. Уголовно-процессуальный кодекс Эстонской Республики (принят 12.02.2003, в редакции от 20.02.2020). URL: http://www.pravo.lv/likumi/29_upz.html.
16. Уголовно-процессуальный кодекс Республики Молдова от 14.03.2003 г. № 122–XV (с изменениями и дополнениями). URL: http://online.zakon.kz/Document/?doc_id=30397729&doc_id2=30397729#pos=30;-15&sub_id2=1020000&sel_link=1001129174.
17. Ратнова А. В. Електронний документ та його місце у системі доказів у кримінальному провадженні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2018. № 3. С. 231–241.
18. Коваленко А. В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник ЛДУВС ім. Е. О. Дідоренка.*2018. Вип. 4(84). С. 237–245.
19. Проект закону "Про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження)" № 9484 від 17.01.2019. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7BG00A.html.
20. Judgment in case of Matanović v. Croatia (application no. 2742/12), 04.04.2017. URL: http://hudoc.echr.coe.int/rus?i=001-172466.

REFERENCES

1. Goodison, Sean E., Davis, Robert C., & Jackson, Brian A. Digital Evidence and the.U.S. Criminal Justice System. Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Retrieved from: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf&ved=2ahUKEwjohpby6tDnAhVFpYsKHW3wB2cQFjAOegQICBAB&usg=AOvVaw1vdoqPLquJerLLqRJLPd-E&cshid=1581676870679.

2. Orin S. Kerr Digital Evidence and the New Criminal Procedure. *Columbia Law Review.* Vol. 105, No. 1 (Jan., 2005), pp. 279–318 Retrieved from: https://www.jstor.org/stable/4099310.
3. Rodriguez, Glen Dario, & Molina, Fernando The preservation of digital evidence and its admissibility in the court. DOI: 10.1504/IJESDF.2017.10002624.
4. Vasyl'yev, S. V., & Nikolenko, L. M. (2004). *Dokazuvannya ta dokazy u hospodars'komu protsesi Ukrayiny* [Evidence and Evidence in the Economic Process of Ukraine]. Monohrafiya. Kharkiv (in Ukr.).
5. Bilousov, A. S. (2008). *Kryminalistychnyy analiz ob'yektiv komp'yuternykh zlochyniv* [Forensic analysis of computer crimes]. Extended abstract of candidate's thesis (12.00.09). Kyiv (in Ukr.).
6. Grigor'yev, O. G. (2003). *Rol' i ugolovno-protsessual'noye znacheniye komp'yuternoy informatsii na dosudebnykh stadiyakh ugolovnogo sudoproizvodstva* [The role and criminal procedural significance of computer information in the pre-trial stages of criminal proceedings]. Extended abstract of candidate's thesis (12.00.09). Omsk (in Russ.).
7. Yegorov, N. N. (2007). *Veshchestvennyye dokazatel'stva: ugolovno-protsessual'nyy i kriminalisticheskiy aspekty* [Physical evidence: criminal procedural and forensic aspects]. Moskva: Yurlitinform (in Russ.).
8. Kuvychkov, S. I. (2016). *Ispol'zovaniye v dokazyvanii po ugolovnym delam informatsii, predstavlennoy v elektronnom vide* [Use in evidence in criminal cases of information provided in electronic form]. Extended abstract of candidate's thesis (12.00.09). Nizhniy Novgorod (in Russ.).
9. Okonenko, R. I. (2016). *Elektronnyye dokazatel'stva i problemy obespecheniya prav grazhdan na zashchitu tayny lichnoy zhizni v ugolovnom protsesse: sravnitel'nyy analiz zakonodatel'stva Soyedinennykh Shtatov Ameriki i Rossiyskoy Federatsii* [Electronic evidence and problems of ensuring the rights of citizens to protect privacy of a criminal process: a comparative analysis of the laws of the United States of America and the Russian Federation]. Extended abstract of candidate's thesis (12.00.09). Moskva (in Russ.).
10. Sekhan, D. M. (2013). Tsyfrovi dokazy: ponyattya, osoblyvosti ta mistse v systemi dokazuvannya [Digital Evidence: Concepts, Features, and Place in the Evidence System]. *Naukovyy visnyk Mizhnarodnoho humanitarnoho universytetu. Ser.: Yurysprudentsiya,* (5). 256–260 (in Ukr.).
11. Zigura, N. A., & Kudryavtseva, A. V. (2011). *Komp'yuternaya informatsiya kak vid dokazatel'stv v ugolovnom protsesse Rossii* [Computer information as a type of evidence in the criminal process of Russia]. Monografiya. Moskva: Yurlitinform (in Russ.).
12. Ivanov, N. A. (2015). *Dokazatel'stva i istochniki svedeniy v ugolovnom protsesse: problemy teorii i praktiki* [Evidence and sources of information in criminal proceedings: problems of theory and practice]. Monografiya. Moskva: Yurlitinform (in Russ.).
13. Metelev, O. P. (2018). Hnoseolohichna ta pravova pryroda tsyfrovykh dokaziv u kryminal'nomu protsesi [The epistemological and legal nature of digital evidence in criminal proceedings]. *Pravova pozytsiya,* 1(20). 75–86 (in Ukr.).
14. Kryts'ka, I. O.; Tumanyants, A. R. (Red.). (2018). *Rechovi dokazy u kryminal'nomu provadzhenni* [Material evidence in criminal proceedings]. Monohrafiya. Kharkiv: Pravo (in Ukr.).
15. *Ugolovno-protsessual'nyy kodeks Estonskoy Respubliki* [Code of Criminal Procedure of the Republic of Estonia]. (12.02.2003 v redaktsii ot 20.02.2020). Retrieved from: http://www.pravo.lv/likumi/29_upz.html (in Russ.).
16. *Ugolovno-protsessual'nyy kodeks Respubliki Moldova* [Code of Criminal Procedure of the Republic of Moldova]. (14.03.2003. No 122–15). Retrieved from: http://online.zakon.kz/Document/?doc_id=30397729&doc_id2=30397729#pos=30;-15&sub_id2=1020000&sel_link=1001129174 (in Russ.).
17. Ratnova, A. V. (2018). Elektronnyy dokument ta yoho mistse u systemi dokaziv u kryminal'nomu provadzhenni [An electronic document and its place in the system of evidence in criminal proceedings]. *Naukovyy visnyk L'vivs'koho derzhavnoho universytetu vnutrishnikh sprav. Seriya yurydychna,* (3). 231–241 (in Ukr.).
18. Kovalenko, A. V. (2018). Elektronni dokazy v kryminal'nomu provadzhenni: suchasnyy stan ta perspektyvy vykorystannya [Electronic Evidence in Criminal Proceedings: Current State and Prospects for Use]. *Visnyk LDUVS im. E. O. Didorenka,* 4(84). 237–245 (in Ukr.).
19. *Proekt zakonu "Pro vnesennya zmin do Kryminal'noho protsesual'noho kodeksu Ukrayiny ta Kryminal'noho kodeksu Ukrayiny (shchodo vdoskonalennya poryadku zastosuvannya okremykh zakhodiv zabezpechennya kryminal'noho provadzhennya)"* [Draft Law "On Amendments to the Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine (on Improving the Procedure for the Application of Certain Measures to Ensure Criminal Proceedings)"]. (17.01.2019 No. 9484). Retrieved from: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7BG00A.html (in Ukr.).

20. Judgment in case of Matanović v. Croatia (application no. 2742/12), 04.04.2017. Retrieved from: http://hudoc.echr.coe.int/rus?i=001-172466.

ІНФОРМАЦІЯ ПРО СТАТТЮ (ARTICLE INFO)

Published in:
Форум права: 60 pp. 37–46.

Related identifiers:

10.5281/zenodo.3577546

http://forumprava.pp.ua/files/037-046-2020-1-FP-Demura,Klepka,Krytska_7.pdf

http://nbuv.gov.ua/UJRN/FP_index.htm_2020_1_7.pdf

License (for files):
Creative Commons Attribution 4.0 International

Received: 22.01.2020
Accepted: 21.02.2020
Published: 26.02.2020

Cite as:

Демура, М. І., Клепка, Д. І., & Крицька, І. О. (2020). Щодо обмеження прав особи під час вилучення цифрових джерел доказової інформації у кримінальному провадженні. *Форум Права,* 60(1). 37–46. DOI: http://doi.org/10.5281/zenodo.3577546.

Demura, M. I., Klepka, D. I., & Krytska, I. O. (2020). Shchodo obmezhennya prav osoby pid chas vyluchennya tsyfrovykh dzherel dokazovoyi informatsiyi u kryminal'nomu provadzhenni [Restriction of Personal Rights When Removing Digital Sources of Evidence in Criminal Proceedings]. *Forum Prava,* 60(1). 37–46. DOI: http://doi.org/10.5281/zenodo.3577546.

Форум права Форум права Форум права