РОЗДІЛ 8. КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 341.1
DOI https://doi.org/10.24144/2307-3322.2022.75.2.23

ПРАВОВА РЕГЛАМЕНТАЦІЯ ЕЛЕКТРОННИХ ДОКАЗІВ ТА ПРАКТИКА ЇХ ВИКОРИСТАННЯ В СУДОЧИНСТВІ УКРАЇНИ

Ахтирська Н.М.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу та криміналістики
Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка
Akhtyrska.n@gmail.com
https://orcid.org/0000-0003-3357-7722

Ахтирська Н.М. Правова регламентація електронних доказів та практика їх використання в судочинстві України.

В статті на підставі аналізу судової практики (кримінальне, цивільне, адміністративне та господарське судочинство) аналізується оцінка та використання судами доказів, одержаних в електронному виді, та робиться висновок щодо відсутності одностайності у цих питаннях; зокрема, щодо самого поняття «електронний доказ» (в Кримінальному процесуальному кодексі України, на відміну від інших процесуальних кодексів, даний термін не визначено) та його дублікату чи копії, способу фіксації та посвідчення (ким: провайдером чи іншим суб'єктом), використання судом скріншоту тощо. Підписання Україною 30 листопада 2022 року Другого додаткового протоколу до Конвенції про кіберзлочинність, який скерований на удосконалення процесу збору електронних даних, покладає початок нового законотворчого процесу щодо удосконалення національного законодавства України відповідно до міжнародних стандартів. Підґрунтям для цього є створена правова основа для міжнародного прямого співробітництва з постачальниками послуг, прискорених форм співробітництва для розкриття інформації про абонента та дані трафіку, прискореного співробітництва та розкриття інформації у надзвичайних ситуаціях, також передбачені додаткові інструменти взаємної допомоги, захист даних та інші гарантії верховенства права, вперше дається визначення «надзвичайної ситуації», під якою слід розуміти ситуацію, що створює значний та неминучий ризик для життя або безпеки будь-якої фізичної особи, а «персональними даними» вважається інформація, що має відношення до ідентифікації особи. Пропонується на підставі оновлених міжнародних стандартів, чинного законодавства та практики започаткувати глибинне дослідження «Теорія електронних доказів», що сприятиме розробці вивірених законопроектів та ухвалення парламентом закону, в якому наводились би однозначні терміни «електронний доказ», копія /дублікат електронного доказу, порядок вилучення, фіксації чи посвідчення, повноваження провайдера у сприянні судочинству.

Ключові слова: електронний доказ, комп'ютерні дані, персональні дані, надзвичайна ситуація, копія/дублікат доказу в електронному виді.

Akhtyrska N. Legal regulation of electronic evidence and the practice of their use in the judiciary of Ukraine.

The article, based on the analysis of judicial practice (criminal, civil, administrative and economic proceedings), analyzes the assessment and use of evidence received in electronic form by courts, and draws a conclusion regarding the lack of unanimity in these issues; in particular, regarding the very concept of "electronic evidence" (in the Criminal Procedural Code of Ukraine, unlike other procedural codes, this term

is not defined) and its duplicate or copy, the method of recording and certification (by whom: by the provider or another entity), the use screenshot seizure, etc. Ukraine's signing on November 30, 2022 of the Second Additional Protocol to the Convention on Cybercrime, which is aimed at improving the process of electronic data collection, marks the beginning of a new law-making process to improve Ukraine's national legislation in accordance with international standards. The basis for this is the created legal basis for international direct cooperation with service providers, accelerated forms of cooperation for disclosure of information about the subscriber and traffic data, accelerated cooperation and disclosure of information in emergency situations, additional tools for mutual assistance, data protection and other guarantees of the rule of law are also provided, the definition of "emergency situation" is given for the first time, which should be understood as a situation that creates a significant and unavoidable risk to the life or safety of any natural person, and "personal data" is considered to be information related to the identification of a person. On the basis of updated international standards, current legislation and practice, it is proposed to start an in-depth study of the "Theory of electronic evidence", which will contribute to the development of verified bills and the adoption by the parliament of a law that would specify the unambiguous terms "electronic evidence", a copy/duplicate of electronic evidence, the order of withdrawal, records or certificates, the provider's authority to assist in legal proceedings.

Key words: electronic evidence, computer data, personal data, emergency situation, copy/duplicate of evidence in electronic form.

Вступ. Розвиток науки та техніки створив необмежені можливості для цивілізаційного розвитку та одночасно сприяв виникненню суттєвих для неї загроз. Цифровізація, комп'ютерізація, електронний документообіг та банкінг, інформаційні бази даних стали зручним інструментом сучасного світу, проте, як свідчать статистичні показники, загрозливими темпами зростає кількість злочинів, що вчиняються з використанням інформаційних технологій. За даними ФБР, щорічні втрати від розробки шкідливих програм становлять 1 трлн. дол. (для порівняння, вартість Microsoft станом на квітень 2021 року складала 1, 9 млрд. дол.) [1]. Визнаним є факт, що боротьба з такими злочинами перебуває у прямій залежності від інформаційно-технологічного забезпечення, втім, цього не достатньо – потребує ґрунтовного переосмислення теорія доказів. Йдеться про визначення певних категорій, як то «електронний доказ», «цифровий доказ», «оригінал електронного чи цифрового документу», «копія електронного чи цифрового документу», матеріальний носій інформації (у випадку перебування даних в «хмарних» сховищах), також доцільно регламентувати способи одержання такої інформації від державних органів, приватних компаній, провайдерів, фізичних осіб, удосконалити чинне законодавство щодо оперативного міжнародного співробітництва у кримінальному провадженні. Кожна держава визначає національні вимоги до визнання доказі достовірними, зокрема, в Законі Індії «Про електронні докази» (2000р.) йдеться про необхідність доведення ліцензійності програми (продукту), який містить інформацію. Очевидно, що такий підхід вирішує проблему боротьби з контрафактними інформаційними програмами [2]. Barbara Halasek, Head of Regulatory Affairs [3], James D. Shaw, Senior Legal Officer, UNICRI [4], Maria Orav [5] та інші вчені розкрили сутність та можливості використання електронних доказів та виклики, які стоять перед законодавцями держав, під час міжнародного заходу, що відбувся для співробітників фінансової розвідки 8-9 листопада 2021 року.

Мета дослідження. На підставі аналізу судових рішень у різних видах судочинства продемонструвати неодностайність судової практики щодо оцінки та використання електронних доказів, з урахуванням підписання Україною Другого додаткового протоколу до Конвенції про кіберзлочинність внести пропозиції щодо розробки теорії електронних доказів та прийняття спеціального закону, яким би регламентувалась процедура використання електронних доказів.

Викладення основного матеріалу. Перш за все варто визначити природу слідів чи інформації, якою оперують експерти у галузі боротьби з кіберзлочинами («цифровий слід», «цифрова ідентифікація», «ланцюжок кримінальних цифрових операцій», «цифрова інформація для ідентифікації особи (злочинця)», «цифровий портрет злочинця» тощо). Варто визнати, що електронна комунікація використовується особами для підготовки, вчинення та приховання слідів злочину, інформаційні можливості сприяють створенню електронних документів, поширенню тощо. Відповідно до Закону України «Про електронні документи та електронний документообіг», електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа (ст. 5), оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним

до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги». У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу (ст. 7), юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму, а допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму (ст. 8) [6]. Законом України «Про електронні комунікації» визначено, що електронна комунікація (телекомунікація) - передавання та/або приймання інформації незалежно від її типу або виду у *вигляді електромагнітних сигналів* за допомогою технічних засобів електронних комунікацій [7]. Традиційно в криміналістиці виділяють два види слідів – матеріальні та ідеальні, що визначило й процесуальний порядок їх виявлення, фіксації, вилучення, дослідження та використання в кримінальному провадженні. З огляду на наведені визначення, електронна інформація має ознаки матеріального сліду, оскільки зберігається на матеріальних носіях та може бути вилучена. Комп'ютер, принцип дії якого хоча й має певну подібність з принципом дії людського мозку, суттєво відрізняється від нього хоча б тим, що складається не з нейронів, а з електронних схем. З іншого боку, електронній інформації притаманні ознаки ідеального сліду, оскільки вона циркулює у вигляді *електромагнітних сигналів,* вона невидима, не сприймається за допомогою зору, слуху та збільшувальних приладів та магнітних порошків тощо. В комп'ютері має обов'язково бути два процеси: кодування та декодування. Тож для візуального сприйняття електронна інформація має бути виведена на монітор, або перенесена на матеріальний носій. Електронній інформації притаманні й власні ознаки, відмінні від матеріальних та ідеальних: 1) електронна інформація може зберігатися не на всіх матеріальних об'єктах, а лише в пам'яті комп'ютера та інших спеціальних носіях; 2) під час копіювання електронної інформації джерело не зазнає будь-яких змін (за виключенням випадків використання шкідливих програм), термін копіювання до електронної інформації визнається неточним, оскільки відповідна дія є дублюванням або клонуванням.

Нематеріальна природа будь-яких даних та інформації, що зберігаються в електронному вигляді, значно полегшує маніпуляції та є більш схильною до змін, ніж традиційні форми доказів. Це створює особливі виклики для системи правосуддя, яка вимагає, щоб такі дані оброблялися певним чином, щоб забезпечити цілісність доказів, які надаються в межах проваджень. Зважаючи на унікальні характеристики, електронні докази міжнародні експерти визначають як «*будь-яку інформацію, що генерується, зберігається або передається в цифровій формі, яка згодом може знадобитися для підтвердження або спростування факту, оскаржуваного в межах провадження*». Попри те, що в різних юрисдикціях подробиці можуть відрізнятися, загалом під час оцінювання електронних доказів для судового розгляду слід враховувати такі критерії: 1) *автентичність* (факти повинні встановлюватись на основі доказів таким чином, щоб їх не можна було оскаржити; крім того, вони повинні засвідчувати їхній початковий стан); 2) *повнота* (аналіз чи будь-який висновок, який ґрунтується на свідченнях, повинен розповідати всю історію, а не підлаштовуватися під більш сприятливу чи бажану точку зору); 3) *надійність* (не можна збирати та представляти докази жодним чином, який може поставити під сумнів їхню достовірність або правдивість); 4) *переконливість* (докази повинні доводити факти, які вони засвідчують, а фахівці, на яких покладено завдання щодо встановлення фактів у межах судового процесу, повинні мати можливість покладатися на них як на правду); 5) *пропорційність* (методи, які використовуються для збирання доказів, повинні бути справедливими та пропорційними інтересам справедливості (упередженість (тобто рівень вторгнення чи примусу) щодо прав будь-якої сторони не повинна переважати над «доказовою цінністю» доказів (тобто їхньої цінністю як доказу) [8].

Нерозробленість теорії цифрових доказів призводить до певних труднощів, з якими стикаються правоохоронні органи та суди. Зокрема, предметом оскарження стало питання про використання інформації з цифрових відеокамер (скаржник посилався на недопустимість доказів, одержаних з цифрових відеокамер спостереження без дозволу суду на тимчасовий доступ). Кримінальний касаційний суд не погодився з доводами у касаційній скарзі про те, що відеозапис з камер спостереження отримано у позапроцесуальний спосіб, оскільки, як вбачається з матеріалів кримінального провадження, відеозапис з камер внутрішнього спостереження ресторану було *добровільно надано* директором цього закладу на запит слідчого. Відповідно до ст. 93 КПК України, сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, *витребування та отримання* від органів державної влади, органів місцевого самоврядування, підпри-

ємств, установ та організацій, службових та фізичних осіб, речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом. В рамках кримінального провадження правом витребувати від будь-якої особи необхідні речі, документи, відомості, тощо, наділений слідчий. Ураховуючи викладене, звернення до слідчого судді для отримання ухвали про тимчасовий доступ до відповідних документів в даному випадку не є обов`язковим [9]. При розгляді кримінальних проваджень аналогічної позиції дотримуються суди щодо цифрової інформації, одержаної з Kyiv Smart City [10].

Значний обсяг доказової інформації міститься в мобільних телефонах, то ж чи має право слідчий читати текстові повідомлення без ухвали слідчого судді? Верховний Суд відзначив, що безпідставним є твердження про те, що під час досудового розслідування було здійснено незаконний (без ухвали слідчого судді) доступ до відомостей з електронних інформаційних мереж, який оформлено як *протокол огляду предмета – телефону.* Сутність такої негласної слідчої (розшукової) дії, як доступ до зняття інформації з електронних інформаційних систем, полягає у здійсненні на підставі ухвали слідчого судді пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частин, доступ до яких обмежений власником, володільцем або утримувачем системи розміщенням її у публічно недоступному місці, житлі чи іншому володінні особи або логічним захистом доступу, а також отримання таких відомостей без відома її власника, володільця або утримувача. Зняття інформації з електронних інформаційних систем або їх частин можливе без дозволу слідчого судді, якщо доступ до них не обмежується їх власником, володільцем або утримувачем або не пов`язаний з подоланням системи логічного захисту. Стосовно інформації, яка була наявна в мобільному телефоні засудженого, то вона була досліджена шляхом включення телефону та огляду текстових повідомлень, які в ньому знаходились та доступ до яких не був пов'язаний із наданням володільцем відповідного серверу (оператором мобільного зв'язку) доступу до електронних інформаційний систем. У даному випадку орган досудового розслідування провів огляд предмета - телефона та оформив його відповідним протоколом, який складений з дотриманням вимог кримінального процесуального закону. За таких обставин ВС не виявив порушень вимог Кримінального процесуального кодексу України [11].

ККС ВС висловився й щодо особливостей *збирання та подання доказів* у кримінальному провадженні. Правова природа подання доказів є іншою, ніж одержання їх шляхом проведення слідчих дій, оскільки подання доказів має наслідком їх отримання, що полягає у прийманні того, що надсилається, надається або вручається, тобто при отриманні певна особа добровільно передає, надає, представляє матеріали слідчому чи прокурору. При отриманні предметів та документів, представлених особою для залучення їх до справи як доказів, орган дізнання, слідчий або суд повинні допитати особу, яка подає даний предмет чи документ, з метою з'ясування джерела та обставин їх отримання, потім здійснити огляд цих предметів або документів і процесуально зафіксувати їх отримання. Так, вироком Красногвардійського районного суду особу визнано винуватим у скоєнні злочину, передбаченого ч. 2 ст. 185 КК України. Ухвалою Дніпровського апеляційного суду вирок залишено без змін. У касаційній скарзі захисник зазначив, що суд апеляційної інстанції залишив поза увагою *недопустимість таких доказів як копія диску відеозапису з камер відеоспостереження*, вказав на відсутність протоколу тимчасово вилученого майна. Відповідно до ст. 86 КПК доказ визнається допустимим, якщо він отриманий в порядку встановленому КПК. Недопустимий доказ не може бути використаний при прийнятті процесуальних рішень, на нього не може посилатися суд при ухваленні судового рішення. Згідно ст. 87 КПК докази, отримані внаслідок здійснення процесуальних дій, які потребують попереднього дозволу суду, без такого дозволу є недопустимими. Відповідно до ч. 3 ст. 214 КПК здійснення досудового розслідування до внесення відомостей до реєстру або без такого внесення не допускається і тягне за собою відповідальність, установлену законом. Згідно частин 1 та 2 ст. 93 КПК, збирання доказів здійснюється сторонами кримінального провадження, потерпілим, представником юридичної особи, щодо якої здійснюється провадження, у порядку, передбаченому цим Кодексом. Сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) та негласних слідчих (розшукових) дій, витребування та одержання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом. Збирання доказів, у тому числі й речових, відбувається через інститут слідчих дій. Відповідно до ч. 1 ст. 223 КПК саме слідчі (розшукові) дії є діями, спрямованими на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні. Зазначене узгоджується з висновком Верховного Суду, викладеним у постанові від 31

березня 2021 року у справі № 333/1539/16-к. У цьому контексті потрібно зазначити, що відеозапис з місця події був вилучений не шляхом проведення слідчої дії, а шляхом *збирання речових доказів*, зокрема, подання відеодиску з копією відеозапису з місця події особою, яка не має зацікавленості в даній кримінальній справі. Правова природа подання доказів є іншою, ніж одержання їх шляхом проведення слідчих дій, оскільки подання доказів має наслідком їх отримання, що полягає у прийманні того, що надсилається, надається або вручається, тобто при отриманні певна особа добровільно передає, надає, представляє матеріали слідчому чи прокурору. При отриманні предметів та документів, представлених особою для залучення їх до справи в якості доказів, орган дізнання, слідчий або суд повинні допитати особу, яка подає даний предмет чи документ, з метою з`ясування джерела та обставин їх отримання, потім здійснити огляд цих предметів або документів і процесуально зафіксувати їх отримання. Як вбачається з матеріалів кримінального провадження, свідок добровільно та за власною ініціативою надав слідчому зазначений диск з відеозаписом з камер відеоспостереження. Колегія суддів Верховного Суду погодилась з апеляційним судом, що відсутні правові підстави, вважати, що зазначений відеозапис з камер спостереження, який був переглянутий судом першої інстанції у судовому засіданні, є не допустимим доказом, оскільки диск з відеозаписом добровільно надав свідок, факт чого останній безпосередньо підтвердив в судовому засіданні, а тому надання цього диску з відеозаписом безпосередньо свідком, не можна вважати порушенням вимог ст. 93 КПК [12].

Неодноразово предметом дискусій серед науковців та практиків було питання щодо суб'єкту збору та надання доказів. Черговий раз постало питання щодо допустимості у якості доказу розмови, зафіксованої на диктофон мобільного телефону. Верховний Суд розглянув справу, в якій досліджував питання допустимості як доказу запису телефонної розмови, зробленого на диктофон мобільного телефону засудженого. Засуджений під час розмови зі свідком повідомив, що саме він вбив потерпілу. У судовому засіданні свідок підтвердила обставини телефонної розмови із засудженим і її зміст. Доводи касаційної скарги захисника щодо недопустимості як доказу запису телефонної розмови, зробленого на диктофон мобільного телефону, оскільки стороною обвинувачення не було доведено автентичності голосу засудженого, колегія суддів Верховного Суду визнала безпідставними та необґрунтованими, оскільки у ході судового розгляду в суді першої інстанції було відтворено запис телефонної розмови, зробленої на диктофон мобільного телефону засудженого, який він добровільно видав після його затримання. Разом з тим у ході дослідження вказаного доказу місцевим судом встановлено, що засуджений під час розмови зі свідком повідомив, що саме він вбив потерпілу. При цьому сама свідок у судовому засіданні підтвердила обставини телефонної розмови з засудженим та її зміст. Відповідно до вироку місцевий суд, врахувавши вказані обставини, дійшов висновку, що досліджений доказ згідно з нормами ст. 86 КПК України є законним та допустимим з урахуванням того, що засуджений не заперечував, що виданий ним телефон належить саме йому і він особисто використовував програму для запису телефонної розмови на диктофон. Разом з тим місцевий суд спростував доводи сторони захисту щодо автентичності голосу засудженого на аудіо-записі, посилаючись на те, що клопотання про призначення та проведення фоноскопічної експертизи щодо ідентифікації голосів осіб, між якими відбулася розмова, стороною захисту заявлено не було. При цьому підстав, які б вказували на неналежність цього запису як доказу, судом першої інстанції не встановлено. З цією позицією суду першої інстанції погодилась і колегія суддів [13].

Неоднозначним є тлумачення судами таких понять як «копія» та «дублікат», також дискусійним є питання щодо поширення такого тлумачення щодо письмових (паперових) носіїв на цифрові джерела інформації. Так, згідно з обвинувальним актом особи з використанням наданої їм влади і службового становища, всупереч інтересам служби, одержували від суб`єктів підприємницької діяльності на системній основі неправомірну вигоду за безперешкодне повернення та не створення умов по перешкоджанню повернення бюджетного відшкодування податку на додану вартість. Крім цього, з метою отримання неправомірної вигоди та незаконного збагачення організували та створили умови, за яких суб`єкти підприємницької діяльності за формальне проведення документальної перевірки підприємницької діяльності та зменшення податкових зобов`язань перед державою змушені були передавати службовим особам неправомірну вигоду ч. 3 ст. 368 КК України). Ухвалою Волинського апеляційного суду виправдувальний вирок Луцького міськрайонного суду Волинської області залишено без змін. У касаційній скарзі прокурор, посилався на те, що судом не дотримано засад змагальності кримінального процесу, а також порушено право сторони обвинувачення на обстоювання правової позиції, що, в силу статей 412, 438 КПК є істотним порушенням вимог кримінального процесуального закону. На його переконання, судом апеляційної інстанції безпідставно відмовлено стороні обвинувачення у

задоволенні клопотання про дослідження недосліджених доказів, а саме клопотань, ухвал та протоколів за результатами проведення негласних слідчих (розшукових) дій, ухвали слідчого судді, протоколів огляду місця події та допиту свідків, метою яких було встановлення обставин, з`ясування яких має суттєве значення для ухвалення законного, обґрунтованого та справедливого рішення. Прокурор стверджував, що протоколи проведення НСРД, матеріальні носії інформації, на яких містилась інформація щодо їх проведення є дублікатами, а не копіями, що не перешкоджає визнанню їх судом як оригіналів документів. Щодо посилання прокурора на порушення, допущене судом апеляційної інстанції в частині відмови у долучені та дослідженні протоколів за результатами проведення НСРД з додатками, колегія суддів Верховного Суду виходила з наступного. У чинному КПК використовуються такі терміни як «дублікат документа» (частина 4 статті 99 КПК) та «копія документа». З огляду на прийняті судові рішення, суди першої та апеляційної інстанції розглядають ці терміни як *слова-синоніми*. Так, суд першої інстанції у вироку зазначає: «В судовому засіданні прокурор клопотав про дослідження та долучення до матеріалів вказаного кримінального провадження та визнання їх доказами оригіналів клопотань про проведення негласних слідчих розшукових дій, оригіналів ухвал апеляційного суду Волинської області про надання дозволів на проведення таких негласних слідчих розшукових дій, а також копій (дублікатів) протоколів НСРД і копій (дублікатів) дисків до них». Суд апеляційної інстанції в ухвалі вказує: «Що стосується доводів апеляційної скарги про порушення судом першої інстанції вимог ст. 99 КПК України, то слід зазначити, що місцевим судом правильно встановлено, що копії (дублікати) протоколів НСРД та дисків до них, є *недопустимими* та не можуть бути дослідженими судом, так як вимогами ч. 3 ст. 99 КПК України передбачено, що сторона кримінального провадження зобов`язані надати суду оригінал документа. Проте вказані документи не є оригіналами і отримані в іншому кримінальному провадженні». Колегія суддів ВС не погодилась з таким підходом з огляду на «Національний стандарт України. Діловодство й архівна справа. Терміни та визначення понять. ДСТУ 2732:2004», якому надано чинності наказом Державного комітету України з питань технічного регулювання та споживчої політики України від 28 травня 2004 року № 97 «Про затвердження національних стандартів України, державних класифікаторів України, національних змін до міждержавних стандартів, внесення зміни до наказу Держспоживстандарту України від 31 березня 2004 р. № 59 та скасування нормативних документів» (далі – ДСТУ 2732:2004). Відповідно до пункту 3.10 ДСТУ 2732:2004 *копія (документа)* – це документ, шо містить точне знакове відтворення змісту чи документної інформації іншого документа і в окремих випадках – деяких його зовнішніх ознак. Згідно з пунктом 3.14 ДСТУ 2732:2004, *дублікат оригіналу* (службового документа) – це повторно оформлений службовий документ для використовування, замість втраченого чи пошкодженого оригіналу, що має таку саму юридичну силу. Таким чином, терміни «копія» і «дублікат» не є синонімічними. Разом з тим, слід зазначити, що КПК у частині 4 статті 99 надає автономне визначення поняття «дублікат документа» як документа, виготовленого таким самим способом, як і його оригінал. Отже, для точного використання даних термінів у кримінальній процесуальній діяльності термін «копія документа» слід визначати за пунктом 3.10 ДСТУ 2732:2004, а термін «дублікат документа» – за частиною 4 статті 99 КПК. Враховуючи, що під документом як джерелом доказів законодавець розуміє 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, у тому числі матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні), складені в порядку, передбаченому КПК, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії, (частина 1, пункти 2, 3 частини 2 статті 99 КПК), колегія суддів ВС дійшла висновку, що не вбачає жодних перепон *у можливості надання до суду дублікатів протоколів процесуальних дій, а також матеріалів фотозйомки, звукозапису, відеозапису та інших носіїв інформації (у тому числі електронних), виготовлених слідчим, прокурором із залученням спеціаліста, які визнаються судом як оригінал документа.* З огляду на зазначене вище, Верховний Суд дійшов висновку, що посилання судів першої та апеляційної інстанції на положення частини 3 статті 254 КПК в редакції, яка діяла до внесення до неї змін відповідно до Закону України № 187-IX від 04 жовтня 2019 року, є безпідставним [14].

В іншому провадженні Верховний Суд уточнив попередню позицію, зокрема, зазначив, що диски є способом збереження інформації з електронного документа, головною особливістю якого є відсутність жорсткої прив'язки до конкретного матеріального носія. Згідно із Законом України «Про електронні документи та електронний документообіг» (ст. 5), ДСТУ 7157:2010, затвердженого наказом

Державного комітету України з питань технічного регулювання та споживчої політики від 11.03.2010 № 8 «Інформація та документація. Видання електронні. Основні види та вихідні відомості», електронним є документ, де інформація подана у формі електронних даних і для використання якого потрібні засоби обчислювальної техніки. *Диски як матеріальні носії є способом збереження інформації з електронного документа, головною особливістю якого є відсутність жорсткої прив'язки до конкретного матеріального носія, де оригінал електронного документа може існувати на різних носіях, оскільки відповідно до ст. 7 Закону України «Про електронні документи та електронний документообіг» у випадку його зберігання на кількох електронних носіях інформації кожних з електронних примірників вважається оригіналом електронного документа [15].*

Верховним Судом надано роз'яснення щодо використання інформації, яка передається за допомогою Viber, та чи є вона належним електронним доказом. Жінка, яка проживає з дитиною в Словацькій Республіці, просила суд заборонити колишньому чоловіку вести листування й телефонні переговори, на підтвердження вимог вона надала скріншоти повідомлень з телефону та планшету, роздруківки з Viber. У переписці, яку екс-чоловік веде телефоном із заявником з приводу організаційних побачень з сином, він вдається до відкритих погроз, образ, приниження честі та гідності, застосовує нецензурну лайку, називає непристойними словами заявника, її родичів, вживає лексику, недопустиму у нормальному людському спілкуванні. Протидія насильству у сім`ї є одним із важливих напрямів суспільного розвитку. Вона розглядається не лише як соціальна проблема, а, насамперед, як проблема захисту прав людини і, перш за все, прав жінок. При здійсненні насильства у сім`ї відбувається порушенням прав і свобод конкретної людини, що вимагає втручання з боку держави і суспільства. Невжиття своєчасних обмежувальних заходів щодо кривдника може призвести в подальшому до завдання шкоди здоров`ю потерпілої від насильства у сім`ї. Верховний Суд встановив, що повідомлення в Viber є належним електронним доказом у справі про обмежувальний припис [16].

Електронні пристрої є носіями важливої інформації, яку учасники кримінального провадження мають право надавати суду, водночас в судовій практиці постало питання щодо вигляду таких документів (письмовому, електронному) та порядку посвідчення їх достовірності. Кримінальний процесуальний кодекс України не містить відповіді на дані питання.

Аналіз судової практики свідчить про неодностайне тлумачення електронних доказів та ознак, за якими вони визнаються достовірними, у різних видах судочинства. На думку, Н. Сакари, за загальним правилом роздруківки інтернет-сторінок (вебсторінок) не зараховуються як докази у цивільному судочинстві. Так, КЦС ВС дійшов висновку: «Роздруківки Інтернет-сторінок (вебсторінок), які є паперовим відображенням електронного документа, самі по собі не можуть бути доказом у справі. Такі роздруківки визнаються доказом у разі, якщо вони виготовлені, видані і засвідчені *власником відповідного Інтернет-ресурсу або провайдером, тобто набувають статусу письмового доказу*».

Обґрунтовуючи практику адміністративних судів, Н. Блажівська наводить постанову КАС ВС у справі, в якій відповідачем виступало Держкомтелерадіо. Суд зазначив, що як доказ на підтвердження того, що ТОВ через інтернет-магазин здійснювало розповсюдження ввезених із території Російської Федерації друкованих видань, відповідач до матеріалів справи надав скріншот. Цей знімок підтверджує факт розповсюдження, оскільки містить опис, основні характеристики видавництв, рік видання, ціну книги, умови оплати і доставки, адресу і контакти. КАС ВС резюмував, що такий скріншот є електронним доказом у розумінні ст. 99 КАС України. На думку суддів, якщо такі питання виникають, то юристам починаючи з першої інстанції необхідно звертати увагу на *релевантну судову практику в різних юрисдикціях* та належно мотивувати свою позицію з тим, щоб у суду касаційної інстанції не було потреби скеровувати справу на новий розгляд. Утім, суди приймають як докази скріншоти повідомлень із телефону, планшета, роздруківки з Viber. Окрім того, часто (особливо в трудових справах) роботодавці подають фотографію монітору комп'ютера співробітника для того, щоб довести, що працівник у робочий час займався власними справами. «Фотографія монітору комп'ютера не є електронним доказом, але ця інформація може враховуватися судами за умови, якщо учасник справи не поставить під сумнів надане фото і не попросить надати оригінал», – стверджують судді КЦС ВС [17].

В господарському судочинстві також існують певні особливості тлумачення та використання електронних доказів. Правовий аналіз положень статті 96 Господарського процесуального кодексу України свідчить, що *оригінал електронного доказу* – це первинна інформація в електронній (цифровій) формі, яка містить дані про обставини, що мають значення для справи, та яка є основою для відтворення і копіювання. Чинним законодавством визначено поняття оригіналу електронного документа. *Оригіналом електронного документа*, згідно зі статтею 7 Закону України «Про електронні документи та елек-

тронний документообіг» вважається електронний примірник документа з обов`язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до цього Закону. *Однак законодавством не визначено порядку засвідчення електронних доказів*, зокрема поданих у паперових копіях, ураховуючи також те, що деякі з таких доказів (відео-, звукозаписи) не можуть бути відображені у паперовому виді. Водночас відповідно до частини 2 статті 97 Господарського процесуального кодексу України за клопотанням особи, яка надала суду оригінал електронного доказу на матеріальному носії, суд повертає такий матеріальний носій, на якому міститься оригінал доказу, цій особі після дослідження вказаного електронного доказу, якщо це можливо без шкоди для розгляду справи, або після набрання чинності судовим рішенням, а в матеріалах справи залишається засвідчена суддею копія електронного доказу або витяг з нього. Отже, системний аналіз положень зазначеної статті дає підстави для висновку, що *копії електронних доказів може засвідчувати безпосередньо суддя, але після дослідження оригіналу електронного доказу.* Частиною п`ятою статті 96 Господарського процесуального кодексу України встановлено, якщо подано копію (паперову копію) електронного доказу, суд за клопотанням учасника справи або з власної ініціативи може витребувати у відповідної особи оригінал електронного доказу. Якщо оригінал електронного доказу не поданий, а учасник справи або суд ставить під сумнів відповідність поданої копії (паперової копії) оригіналу, такий доказ не береться судом до уваги. З огляду на викладене, в силу приписів частин третьої та п`ятої статті 96 Господарського процесуального кодексу України праву учасника справи подати до суду паперову копію електронного доказу відповідає право суду витребувати у відповідної особи оригінал електронного доказу з власної ініціативи, зокрема, у випадку, якщо суд ставить під сумнів відповідність поданої копії (паперової копії) оригіналу. При цьому невзяття судом до уваги паперової копії оригіналу електронного доказу є процесуальним наслідком саме неподання оригіналу електронного доказу на вимогу суду (а не неподання його разом із позовом чи відзивом на нього). Відповідно, добросовісно реалізуючи право на подання електронного доказу в його паперовій копії, учасник справи, виходячи з принципу правової визначеності, може розраховувати на відповідні процесуальні дії суду, у випадку виникнення у нього (суду) сумнівів щодо відповідності поданої паперової копії оригіналу, включаючи і право учасника справи, у разі відсутності у нього можливості подати доказ, який витребовує суд, або відсутності можливості подати такий доказ у встановлені строки, повідомити про це суд із зазначенням причин протягом п`яти днів з дня вручення ухвали про витребування таких доказів (частини восьма, десята статті 81 Господарського процесуального кодексу України). Частиною четвертою статті 74 Господарського процесуального кодексу України встановлено, що суд не може збирати докази, що стосуються предмета спору, з власної ініціативи, крім витребування доказів судом у випадку, коли він має сумніви у добросовісному здійсненні учасниками справи їхніх процесуальних прав або виконанні обов`язків щодо доказів [18].

В рамках боротьби з корупцією та порушеннями посадовими особами будь-яких прав громадян, особи стали самостійно фіксувати такі ситуації за допомогою електронних пристроїв, з огляду на це постало питання про правомірність таких дій та використання одержаної інформації у якості доказу. Відповідно до статті 307 Цивільного кодексу України, фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою. Згода особи на знімання її на фото чи відеоплівку припускається, якщо зйомки проводяться відкрито на вулиці, зборах, конференціях, мітингах та інших заходах публічного характеру. Фізична особа, яка погодилася на знімання її на фото-, кіно-, теле- чи відеоплівку, може вимагати припинення їх публічного показу в тій частині, яка стосується її особистого життя. Витрати, пов’язані з демонтажем виставки чи запису, відшкодовуються цією фізичною особо. Знімання фізичної особи на фото-, кіно-, теле- чи відеоплівку, в тому числі таємне, без згоди особи може бути проведене лише у випадках, встановлених законом. У справі, яка розглядалась судом, розмова з лікарем відбулася у робочий час, в його службовому кабінеті. Розуміючи суспільну потребу в будь-якій інформації, отриманій від керівника медичного закладу, щодо додаткових вимог для отримання медичних послуг в умовах пандемії COVID-19, він відкрито записував на мобільний телефон у режимі відеозйомки розмову. Спілкування відбувалося у службовому кабінеті директора комунального закладу, що не є «потенційно чутливим» місцем у розумінні чинного законодавства. Верховний Суд дійшов висновку, що до вказаних правовідносин ст. 307 ЦК України не застосовується, оскільки зйомка на відеоплівку в робочий час, під час виконання посадовою особою своїх службових обов`язків, можлива за відсутності згоди останньої. Тому посилання позивача на ст. 307 ЦК України щодо заборони зйомки без її дозволу під час перебування на робочому місці є необґрунтованими [19].

Отже, поняття електронних доказів потребує подальшого удосконалення з урахуванням стандартів Ради Європи та практики країн ЄС. В Конвенції про кіберзлочинність дається визначення «комп'ютерних даних», що означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою, а також сформульовано поняття «дані про рух інформації», що означає будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, що складала частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір і тривалість комунікації або тип [20]. З урахуванням того, що з часу прийняття Конвенції минуло два десятиліття, змінилось розуміння доказів, виникли потреби швидкого реагування на запити щодо надання інформації у межах міжнародного співробітництва, 17 листопада 2021 року був схвалений Радою Європи Другий додатковий протокол до даної Конвенції, який був відкритий для підписання у березні 2022 року. Україною даний Протокол підписаний 30 листопада 2022 року, що зумовлює його подальшу ратифікацію та внесення відповідних змін до процесуального законодавства. На підставі розроблених рекомендацій доцільно започаткувати розробку наукового проєкту «Теорія електронних доказів», в якому визначити на національному рівні поняття «електронного доказу», носія електронного доказу, копії чи дублікату, способу посвідчення (за потреби), способів збирання тощо та виключити диференційований підхід до визнання достовірності електронних доказів в розрізі видів судочинства.

Список використаних джерел:

1. The Cybersecurity 202: Global losses from cybercrime. URL:https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/ (дата звернення 09.09.2022).
2. Prem Pratap Singh Chauhan. Recent trends in admissibility of electronic evidence: challenges for legal fraternity. URL: https://ujala.uk.gov.in/files/15.pdf (дата звернення 09.09.2022).
3. Barbara Halasek. Sectoral risk assessment of Powering the Mass Adoption of VASPs Blockchain In the New Financial System. URL: https://drive.google.com/drive/folders/1hODFajbRwLQ9nkkTnPjuTrW1EZ_e3ykA (дата звернення 10.11.2022).
4. James D. Shaw. Financial Flows in the EU Eastern Partnership Region. 3 December 2021. URL: https://drive.google.com/drive/folders/1hODFajbRwLQ9nkkTnPjuTrW1EZ_e3ykA (дата звернення 10.11.2022).
5. Maria Orav. Lessons learnt from the Estonian assessment of VASPs. URL: https://drive.google.com/drive/folders/1hODFajbRwLQ9nkkTnPjuTrW1EZ_e3ykA (дата звернення 10.11.2022).
6. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 року. URL: https://zakon.rada.gov.ua/laws/show/851-15/card2#Card (дата звернення 10.11.2022).
7. Закон України «Про електронні комунікації» від 16.12.2020 року. URL: https://zakon.rada.gov.ua/laws/show/1089-20#n2246 (дата звернення 10.11.2022).
8. Handbook on Electronic Evidence. Basic Handbook for Law Enforcement Assistants, Prosecutors and Judges. Version 2.1. Cybercrime Division Directorate-General for Human Rights and the Rule of Law Strasbourg, France. March 6, 2020.
9. Постанова ККС ВС від 6 жовтня 2020 року. Справа № 761/480/19. Провадження № 51 - 836 км 20. URL: https://reyestr.court.gov.ua/Review/92173613 (дата звернення 10.11.2022).
10. Постанова Київського апеляційного суду від 11 червня 2021 року. URL: https://reyestr.court.gov.ua/Review/97759360 (дата звернення 10.11.2022).
11. Постанова ВС від 09 квітня 2020 року. URL: https://reyestr.court.gov.ua/Review/88749345?fbclid=IwAR0gdLCRQGS2SjQNaluaOMy8VHgqYwxD0VXB_Cnx5kC38lZihxNj8F1rJrA (дата звернення 10.12.2022).
12. Постанова ВС від 19 травня 2021 року. Справа № 204/4521/18. Провадження № 51-5165 км 20. URL: https://reyestr.court.gov.ua/Review/97134877 (дата звернення 10.11.2022).
13. Постанова ВС від 28 січня 2021 року. Справа № 182/523/16-к. Провадження № 51-1103 км 20. URL: https://reyestr.court.gov.ua/Review/94553286 (дата звернення 12.22 2022). (дата звернення 15.2022).
14. Постанова від 15 січня 2020 р. Справа № 161/5306/16-к. Провадження № 51-3498км19. URL: https://reyestr.court.gov.ua/Review/87053591 (дата звернення 12.12.2022).

15. Постанова ВС від 31 березня 2021 року. Справа № 333/1539/16-к. Провадження № 51-5646км20. URL: https://reyestr.court.gov.ua/Review/96071606?fbclid=IwAR1hhxOPUti0iTZ-W_Af_7OVf3tTMZPXLv7GxElE4Xi75z2vDDqkEPguW6o (дата звернення 15.12. 2022).
16. Постанова ВС від 13 липня 2020 року. Справа №753/10840/19. URL: https://reyestr.court.gov.ua/Review/90385050 (дата звернення 12.12.2022).
17. Судді Верховного Суду поділилися актуальною судовою практикою з питання доказування на підставі електронних доказів. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1155803/ (дата звернення 12.12.2022).
18. Постанова ВС від 23 вересня 2021 року. Справа № 910/17662/19. URL: https://reyestr.court.gov.ua/Review/99818578?fbclid=IwAR3Gf8YkKD1XD_ljuAQ06GRTn6OuQMLqkVDSKRlc3XUK22jiUUuhwB7VaeY (дата звернення 12.12.2022).
19. Рішення Васильківського районного суду Дніпропетровської області від 12.01.2021 року. URL: https://reyestr.court.gov.ua/Review/94117230; Рішення Московського районного суду м. Харкова від 30.08.2019 року // https://reyestr.court.gov.ua/Review/84108554 (дата звернення 12.12.2022).
20. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 12.12.2022).