

SECTION 5.

LAW AND INTERNATIONAL LAW

Фартушко Марія Анатоліївна 

здобувачка вищої освіти факультету прокуратури
Національний юридичний університет ім. Ярослава Мудрого, Україна

Науковий керівник: Колеснікова Інна Анатоліївна 

канд. юрид. наук, доцентка, асистентка кафедри криміналістики
Національний юридичний університет ім. Ярослава Мудрого, Україна

ЕЛЕКТРОННІ ДОКАЗИ: ПРОБЛЕМИ АВТЕНТИЧНОСТІ ТА ДОПУСТИМОСТІ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Стрімкий розвиток інформаційних технологій детермінував перетворення електронних доказів на одну з ключових категорій доказової інформації у кримінальному провадженні. Фактичні дані, зафіксовані в електронній формі, дедалі частіше відіграють вирішальну роль у розслідуваннях, оскільки дослідження цифрових слідів дозволяє об'єктивно встановити хронологію подій, ідентифікувати суб'єктів комунікації, відстежити маршрутизацію даних та зафіксувати факти несанкціонованого втручання в системи. Водночас процес доказування з використанням електронних доказів супроводжується низкою труднощів щодо верифікації їх автентичності, збереження цілісності та забезпечення процесуальної допустимості. Попри те, що кримінальне процесуальне законодавство України закріплює базові засади використання цифрової інформації, правозастосовна практика стикається з об'єктивними перешкодами, що зумовлює необхідність порівняльного аналізу з міжнародними стандартами.

Чинне кримінальне процесуальне законодавство України не містить вичерпного визначення «електронного доказу» саме в межах кримінального процесу, проте загальні положення КПК України дозволяють використовувати як джерело доказів будь-які фактичні дані, одержані в передбаченому законом порядку. Правовий статус електронних документів визначається Законом України «Про електронні документи та електронний документообіг» [1], а верифікація їхнього оригіналу здійснюється шляхом накладення електронного підпису та використання інших інструментів,

передбачених Законом України «Про електронну ідентифікацію та електронні довірчі послуги» [2]. Це створює правове підґрунтя для залучення до процесу доказування електронної кореспонденції, системних журналів (лог-файлів), даних із месенджерів та хмарних середовищ, а також метаданих, що фіксують інформацію щодо дати створення, походження та редагування цифрової інформації.

Попри наявність нормативної-правової бази, ключовою проблемою судової практики залишається верифікація автентичності електронних доказів. З огляду на свою цифрову природу такі файли є вразливими до редагування, причому структурні зміни не завжди залишають очевидні цифрові сліди. Зокрема, електронні копії у вигляді знімків екрана (скріншоти), що часто долучаються учасниками провадження, можуть бути відредагованими, а метадані — цілеспрямовано змінені. Саме тому у вітчизняному судочинстві дедалі більше звертають увагу на так званий «ланцюг володіння» (chain of custody) [3], який передбачає належне процесуальне документування кожного етапу роботи з електронними (цифровими) документами: від моменту їх вилучення до експертного дослідження та судового розгляду. За відсутності безперервності такого ланцюга суд обґрунтовано ставить під сумнів достовірність та допустимість такої доказової інформації.

Дискусійним залишається питання щодо критеріїв визначення «оригіналу» електронного документа. На відміну від традиційних (паперових) носіїв, електронний документ може існувати у кількох ідентичних копіях, а «оригінальність» забезпечується не фізичними характеристиками, а криптографічним захистом, хеш-сумами та системними метаданими. Відповідно до Закону України «Про електронні документи та електронний документообіг», оригіналом електронного документа вважається електронний примірник з обов'язковими реквізитами, зокрема кваліфікованим електронним підписом (КЕП). Однак часто криміналістично значуща інформація міститься не в офіційних документах, а в електронній кореспонденції, мультимедійних файлах, даних месенджерів. У таких випадках верифікація «оригіналу» потребує обов'язкового експертного підтвердження із застосуванням спеціалізованих апаратно-програмних комплексів.

Окрему групу процесуальних та тактичних проблем становить доступ до інформації у хмарних середовищах та на серверах іноземної юрисдикції. Специфіка цифрової інформації полягає в її екстериторіальності: фізична

локалізація даних не завжди корелює з юрисдикційною доступністю, а масиви електронного листування можуть фрагментарно зберігатися в дата-центрах різних країн [4]. За таких умов правоохоронні органи України об'єктивно змушені звертатися до інституту міжнародної правової допомоги, зокрема з використанням механізмів Конвенції про кіберзлочинність (Будапештської конвенції) [5]. Хоча цей міжнародно-правовий акт регламентує процедури взаємодії щодо доступу до електронних доказів, на практиці тривалі строки виконання запитів генерують ризик безповоротної втрати даних через лімітовані періоди зберігання технічної інформації (лог-файлів) провайдерами телекомунікаційних послуг.

Аналіз міжнародного досвіду свідчить, що держави — члени Ради Європи послідовно переходять до моделі технологічної нейтральності в доказовому праві. Цей підхід передбачає відмову від пріоритетності паперових документів над електронними та їх оцінку за єдиними критеріями належності, допустимості й достовірності. У документах Ради Європи акцентується увага на необхідності стандартизації процедур забезпечення ланцюга законного володіння (chain of custody), обчислення контрольних хеш-сум, застосування криптографічного захисту та проведення незалежної комп'ютерно-технічної експертизи. Зі свого боку, Європейський Союз імплементував законодавчий пакет щодо електронних доказів (e-evidence), який оптимізує транскордонний доступ до цифрової інформації, встановлює чіткі строки для виконання запитів провайдерами та підвищує рівень захисту персональних даних. [6]

Для оптимізації вітчизняного кримінального процесу доцільною є імплементация передового міжнародного досвіду, що передбачає: нормативну регламентацію стандартів вилучення електронних носіїв інформації та документування процесів їх дослідження; імперативне застосування криптографічних алгоритмів для підтвердження цілісності даних; підвищення кваліфікації суб'єктів розслідування та експертів у галузі цифрової криміналістики; розбудову мережі спеціалізованих експертних установ; поглиблення міжнародно-правового співробітництва з іноземними провайдерами. Реалізація запропонованого комплексу заходів сприятиме підвищенню доказової цінності цифрової інформації, мінімізації ризиків визнання електронних доказів недопустимими та гармонізації національної правозастосовної практики з європейськими стандартами кримінального судочинства.

Висновки. Слід констатувати, що електронні докази є складним, проте

невід’ємним елементом сучасної системи кримінального судочинства. Їхня доказова цінність залежить не лише від технічних характеристик файлів, а насамперед від неухильного дотримання процесуальних гарантій, законності виявлення та належної процесуальної фіксації. Україна має сформовану нормативно-правову основу для розвитку цифрової криміналістики, а імплементація передового міжнародного досвіду створює дієві механізми для вдосконалення вітчизняної правозастосовної практики. Зазначене є запорукою того, щоб цифрові сліди виступали належними, допустимими та достовірними джерелами доказової інформації у кримінальному провадженні.

Список використаних джерел:

1. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 року, № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>
2. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05 жовтня 2017 року, № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
3. Коваленко В.В. Кримінальний процес України: підручник. — Київ: Юрінком Інтер, 2020. — 720 с.
4. Колеснікова І. А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. Юридичний науковий електронний журнал. № 10. 2023. С. 472–475. URL: http://lsej.org.ua/10_2023/114.pdf
5. Конвенція про кіберзлочинність. Міжнародний документ, ратифікований 07.09.2005 № 2825-IV URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
6. Коваленко В.В. Кримінальний процес України: підручник. — Київ: Юрінком Інтер, 2020. — 720 с.