

Гловюк Ірина Василівна,

професор кафедри кримінального процесу
та криміналістики Одеського державного
університету внутрішніх справ, доктор
юридичних наук, професор

ДЕЯКІ ПИТАННЯ ПРАКТИКИ ККС ВС ЩОДО ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ У ПРОВАДЖЕННЯХ ЩОДО КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

З огляду на специфіку кримінальних правопорушень проти основ національної безпеки, важливим засобом отримання фактичних даних є OSINT. Значення розвідки з відкритих джерел у кримінально-процесуальному контексті досліджується у літературі, зокрема звертається увага на певні практичні проблеми [1–9]. Отже, важливим є виокремлення урахування підходів, які вже сформулював ККС ВС щодо такої інформації, зокрема такої, яка набула властивостей доказів.

Ці підходи доцільно розглянути, виходячи з формулювань ст. 94 КПК України: слідчий, прокурор, слідчий суддя, суд за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожний доказ з позиції належності, допустимості, достовірності, а сукупність зібраних доказів – з позиції достатності та взаємозв'язку для прийняття відповідного процесуального рішення.

Однією з найважливіших позицій ККС ВС, яку викладено в кількох постановках, є така: основними доказами в категорії кримінальних проваджень щодо злочинів проти основ національної безпеки України є електронні (цифрові) докази, до яких належать: матеріали фотозйомки, звуко-запису, відеозапису й інші носії інформації (зокрема комп'ютерні дані), що містяться у відкритих (Інтернет; різноманітні засоби масової інформації; соціальні мережі) чи закритих мережах (приватні месенджери та телеграмканали; особисте листування з використанням комп'ютерної техніки й мобільних телефонів, флешносії, карти пам'яті тощо) [10]. Ця позиція відображає різновиди джерельної бази для доказування, свідчить про визнання важливості доказів з відкритих джерел і відображає специфіку цих та інших електронних доказів саме в цих провадженнях, що цілком релевантно складнощам отримання

доказів, зокрема, у ситуаціях перебування підозрюваних на території держави-терористки російської федерації або на тимчасово окупованих територіях, та діджиталізацією сучасного світу. Крім того, ККС ВС цілком релевантно положенням протоколу Берклі визнав, що сам по собі факт розміщення інформації на відкритих інтернет-ресурсах не свідчить про її недостовірність, якщо така інформація перевірена у встановленому законом порядку та підтверджена іншими доказами [11].

У аспекті *належності доказів* ККС ВС вказував, що «огляди зазначених інтернет-сайтів і телеграм-каналів проведено із дотриманням вимог ст. 237 КПК, зафіксовано (за допомогою функцій скриншоту, друку та запису на технічні носії інформації) зміст відображеної на інтернет-сайтах і в телеграм-каналах як електронних документах інформації, що підтверджує існування обставин, які підлягають доказуванню в цьому кримінальному провадженні. Підстав для визнання вказаних вище протоколів, у яких зафіксовано хід і результати оглядів інтернет-сайтів і телеграм-каналів, недопустимими і неналежними доказами Верховний Суд не вбачає, оскільки ці фактичні дані отримано в порядку, передбаченому КПК» [12]. На проблемність цього формулювання у аспекті розмежування властивостей доказів вже зверталася увага у доктрині [6]. У іншій постанові згадувалася належність доказів [13], утім, спеціальних аргументів щодо неї виокремлено не було.

Допустимість доказів констатується через: деталізацію їх фіксування, зокрема, на основі ст. 237 КПК України та висновки про її відповідність КПК України [10; 12]; належність суб'єкта проведення такого огляду [12; 14]; відкритий характером даних [15]; покликанням на те, що «Суд не має підстав уважати, що інформацію з мережі «Інтернет» було здобуто та здійснено її огляд з порушенням конвенційних або конституційних прав обвинуваченого» (з покликанням на висновок Великої Палати Верховного Суду в постанові від 31 серпня 2022 року (справа № 756/10060/17, провадження № 13-3кс22)) [16]. Крайній аргумент у ситуації цитованої постанови навряд є вдалим, оскільки ККС ВС фактично визнав наявність процесуальних порушень, хоча не відобразив, про які саме порушення йдеться.

Достовірність доказів також оспоровалася у кримінальних провадженнях, хоча і не завжди з прямою згадкою цього терміну. В одному з кримінальних проваджень ККС ВС спростував доводи щодо недостовірності доказів таким чином: колегія суддів вважає непереконливими аргументи захисника про недостовірність даних, отриманих з відкритих джерел засобів масової інформації через

перегляд сторінок мережі Інтернет, посилання на які детально наведені у відповідному протоколі огляду від 6 червня 2022 року, у зв'язку з таким. З метою з'ясування обставин, які підлягають доказуванню, інспектор Управління протидії кіберзлочинам в Одеській області провів огляд публікацій в засобах масової інформації через мережу Інтернет і задля збереження доступності інформації у відкритих джерелах, здійснив її цифрове зберігання – архівацію, яка надає змогу захистити та зберігати інформацію з плином часу, включаючи її справжність, доступність, ідентичність, постійність, рендеринг (візуалізацію) та зрозумілість, що корелюється зі стандартами, викладеними у Протоколах Берклі, визнаних Управлінням ООН (т. 2, а. п. 135–159). Крім цього, інформація зафіксована у згаданому протоколі огляду не суперечить показанням допитаних свідків і протоколу огляду електронних документів від 29 червня 2022 року. Крім цього, сторона захисту не дала жодних відомостей щодо спростування цієї інформації і не навела аргументів, які б вказували на те, що інформація, надана органом досудового розслідування, не відповідає дійсності, зокрема, що вона містить ознаки фальсифікації та/або навмисного спотворення даних [17].

Отже, ККС ВС вже висловив певні позиції щодо тлумачення КПК України у контексті електронних доказів з відкритих джерел у аспекті їх належності, достовірності та допустимості, при цьому визнавши важливий характер таких доказів у провадженнях щодо кримінальних правопорушень проти основ національної безпеки та заперечивши формальний підхід оцінки їх властивостей. Водночас поки що в цій практиці практично немає оцінки дотримання стандартів протоколу Берклі.

Список використаних джерел

1. Пашковський М. І. Цифрова інформація з відкритих джерел. Відкриті цифрові дані у кримінальному провадженні. Концептуальні основи цифровізації кримінального провадження України : монографія / ред. Н. В. Глинська. Харків, 2024. 452 с. DOI: <https://doi.org/10.31359/9786178612139>.

2. Пашковський М. І. Особливості використання OSINT при документуванні та розслідуванні колабораційної діяльності. *Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму* : матеріали Всеукр. науково-практ. конф. (Одеса, 21 лип. 2022 р.). С. 82–86.

3. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. 180 с. URL: <https://doi.org/10.32837/11300.27740>.

4. Нікішев О. В., Тетерятник Г. К. Особливості доказування у кримінальних провадженнях в умовах дії правового режиму воєнного або надзвичайного стану : монографія. Київ : Юрінком Інтер, 2026. 256 с. С. 133–156.

5. Гловюк І. В. Покликання на результати OSINT у вираках щодо воєнних злочинів: шляхи вдосконалення. *Воєнні злочини в сучасних збройних конфліктах: виклики для міжнародного та національного кримінального права* : матеріали круглого столу за участі міжнар. наук.-практ. спільноти (Харків, 23 квіт. 2026 р.) [Електронний ресурс] / редкол. : М. Л. Пахнін, В. Л. Давиденко та ін. Харків : ХНУВС, 2026. С. 150–153. URL: <https://www.researchgate.net/publication/404500479>.

6. Гловюк І. В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2025. Вип. 91: ч. 4. С. 251–259. DOI: <https://doi.org/10.24144/2307-3322.2025.91.4.35>

7. Кульчицька Л. О. Матеріали OSINT як джерела доказів у кримінальних провадженнях за ознаками злочину агресії та воєнних злочинів. *Цифровізація кримінального провадження: стан та перспективи* : матеріали наук.-практ. круглого столу (Харків, 19 верес. 2024 р.). DOI: <https://doi.org/10.31359/9786178411565> С. 97–101.

8. Кудінов С. С., Шехавцов Р. М. Правове регулювання використання OSINT та його результатів під час встановлення обставин кримінальних правопорушень. *Науковий вісник Львівського державного університету внутрішніх справ*. 2025. № 3. С. 126–133. DOI <https://doi.org/10.32782/2311-8040/2025-3-14>.

9. Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порад. / Л. В. Гаврилюк та ін. Київ : ДНДІ МВС України, 2024. 196 с.

10. ЄДРСП. URL: <https://reyestr.court.gov.ua/Review/120838442>.

11. ЄДРСП. URL: <https://reyestr.court.gov.ua/Review/134499602>.

12. ЄДРСП. URL: <https://reyestr.court.gov.ua/Review/129086893>.

13. ЄДРСП. URL: <https://reyestr.court.gov.ua/Review/133475377>.

14. ЄДРСП. URL: <https://reyestr.court.gov.ua/Review/119741340>.

15. ЄДРСП. URL: <https://reyestr.court.gov.ua/Review/132611452>.

16. ЄДРСП. URL: <https://reyestr.court.gov.ua/Review/133475377>.

17. ЄДРСП. URL: <https://reyestr.court.gov.ua/Review/124866093>.