УДК 343.1:303.6(477)
DOI https://doi.org/10.32782/apdp.v105.2025.28

О. О. Торбас

ОСОБЛИВОСТІ ДОКАЗУВАННЯ ЗА ДОПОМОГОЮ OSINT У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Постановка проблеми. «На сьогоднішній день в джерелах масової інформації, в повсякденному житті, в побуті набуває популярність дефініція OSINT» [1, с. 332]. Його можна розглядати як діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору [2]; діяльність по отриманню розвідувальної інформації з відкритих джерел [3]; розвідка на основі аналізу відкритих джерел інформації [4]; діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору, розвідка на основі аналізу відкритих джерел інформації [5]. Однак відсутність єдності в позиціях не означає, що на практиці є реальні суперечки щодо сутності даного поняття. «Необхідно зробити уточнення, що термін «OSINT» є відносно уніфікованим у міжнародній спільноті, який розуміється всіма однаково» [6, с. 7].

На даний момент складно переоцінити значення інформації, отриманої з відкритих джерел, адже переважна більшість населення так чи інакше використовує мережу Інтернет, залишаючи там (інколи навіть не розуміючи цього) цифровий слід. Такі відомості можуть бути використані як в злочинних цілях, так і задля того, щоб викрити осіб, які вчиняють ті або інші правопорушення. Відповідно, детальне вивчення можливостей OSINT у кримінальному процесі на даний момент є вкрай важливою умовою здійснення ефективного досудового розслідування відповідно до сучасних тенденцій. Проте галузь кримінального процесу є однією з найбільш забюрократизованих, адже саме в процесі розслідування, розгляду та вирішення кримінальних правопорушень можуть законно обмежуватися фундаментальні права та свободи людини і громадянина. Через наявність таких ризиків законодавець на рівні нормативного регулювання вводить низку запобіжників задля недопущення зловживання повноваженнями особами, які здійснюють розслідування, розгляд та вирішення кримінальних правопорушень. У зв'язку з цим кримінальне процесуальне законодавство, на жаль, не може швидко пристосовуватися до змін, які відбуваються в суспільстві, в тому числі і щодо використання відомостей, отриманих за допомогою OSINT, в доказуванні. З точки зору нормативного регулювання, всі відомості, отримані з електронних відкритих джерел, в кримінальному процесі розглядаються як документи, отже на них поширюються вимоги, які передбачені ст. 99 КПК України. В той же час такого досить загально положення недостатньо для того, щоб якісно описати всю специфіку використання відомостей, отриманих за допомогою OSINT, в доказуванні.

Аналіз останніх досліджень і публікацій. Проблематикою OSINT переймалися такі вчені як А.В. Білобров, О.В. Дикий, В.В. Сидорчук, П.С. Клімушин та інші. В той же час ці роботи в більшій мірі стосуються специфіка застосування OSINT

в різних сферах, проте майже не стосуються доказування за допомогою даних з відкритих джерел в кримінальному процесі.

Метою статті є визначення недоліків правового регулювання в процесі кримінального процесуального доказування із застосуванням OSINT та формуванн пропозицій щодо подолання таких недоліків.

Виклад основного матеріалу. Існує досить обґрунтована позиція, що відомості, отримані за допомогою OSINT, подібні до відомостей, отриманих оперативним шляхом – вони самі по собі не мають суттєвого доказового значення, проте в сукупності можуть підтверджувати або спростовувати обставини, які підлягають доказуванню у кримінальному процесі. Крім того, до них (на даний момент, виходячи з аналізу судової практики) не ставляться жорсткі вимоги щодо їх допустимості як щодо інших доказів, отриманих шляхом проведення слідчих та негласних слідчих (розшукових) дій, особливо в частині способів їх збирання. Проте твердження про те, що всі такі відомості використовуються як орієнтуюча інформація, також буде помилковим. Так, судова практика свідчить, що відомості, отримані з відкритих електронних джерел, умовно можна поділити на три групи:

1) відомості, які використовуються комплексно з іншими даними, інколи як орієнтуюча інформація. Саме в цій групі найяскравіше проявляється цей зв'язок з оперативно-розшуковою діяльністю. Так, в одному з судових рішень зазначено: «з метою встановлення особи користувача облікового запису месенджера Telegram, а саме «ОСОБА_6», були проведені заходи з розвідки з відкритих джерел (OSINT) та отримано наступну інформацію щодо облікового запису «ІНФОРМАЦІЯ_2»: ID користувача НОМЕР_2, мобільний номер телефону на котрий зареєстрований обліковий запис «ОСОБА_6» НОМЕР_3. За сукупністю зібраних даних, а також відповідно до відомостей ІПНП ОВС України отримано інформацію щодо ОСОБА_8, який причетний до скоєння правопорушення, який зареєстрований та фактично проживає за адресою: АДРЕСА_1» [7]. Відповідно до наданих відомостей слідчий суддя в даному випадку задовольнив клопотання про тимчасовий доступ до речей і документів.

В іншому судовому рішенні зазначено: «за допомогою наявного програмного забезпечення для аналізу даних та інструментів OSINT «ІНФОРМАЦІЯ_20» встановлено, що з використанням електронної скриньки ІНФОРМАЦІЯ_8 було зареєстровано здійснено реєстрацію облікового запису месенджері Skype з іменем ОСОБА_5 та логіном live:.cid.6980f0c320107383. Оперативним шляхом встановлено, що поштові скриньки ІНФОРМАЦІЯ_12 , та ІНФОРМАЦІЯ_13 належать особі ОСОБА_6» [8]. В даному випадку можна помітити, що слідчі обмежуються лише загальними вказівками про використання OSINT, при цьому поєднуючи його зі звичними оперативними методами збору інформацію. На даний момент суддям достатньо такої доказової бази для прийняття відповідних процесуальних рішень. Очевидно, що в більшості випадків мова йде про ті відомості, які відносно легко отримати та перевірити, тому, напевно, судді не ставлять суворі вимоги щодо способу збирання доказів за допомогою OSINT в таких ситуаціях.

2) відомості, що характеризують особу. Наприклад, в одному з рішень зазначається, що «призначаючи покарання обвинуваченій, суд відповідно до вимог

ст. 65 КК України враховує ступінь тяжкості вчиненого кримінального правопорушення, яке відповідно до ст.12 КК України є особливо тяжким злочином (ч. 7 ст. 111-1 КК України), дані про особу винної, те, що вона є громадянкою України, її вік, сімейний та майновий стан, відсутність судимостей (довідка №1-27052024/26006 від 27.05.2024, а.с.147), стан здоров'я (відповідно до листа в.о. директора Департаменту охорони здоров'я Луганської ОВА, за медичною допомогою до закладів охорони здоров'я Луганської області не зверталась, відповідно до листа КНП ЛОР «Центр психічного здоров'я» №729 від 08.06.2024, по медичну допомогу до КНП «ЦПЗ» не зверталась, а.с.135, 136), відповідно до OSINT-аналізу матеріалів про фізичну особу №4/1-2350 від 29.09.2022, була курсанткою Луганського державного університету внутрішніх справ, працювала на посаді поліцейського сектору реагування патрульної поліції у АДРЕСА_2 (а.с.139)…» [9]. Знову таки легкість, з якою можна перевірити цю інформацію, дозволила суду використати її як одну з обставин, що характеризує обвинувачену та може вплинути на призначення покарання.

3) відомості, які напряму стосуються предмету доказування. Власне до таких відомостей повинні ставитись найбільш суворі вимоги в процесі їх оцінки, адже за своїм доказовим значенням вони не будуть відрізнятися від будь-яких інших доказів.

Слід зазначити, що є досить багато прикладів, коли певне процесуальне рішення буде прийнято лише на підставі відомостей, отриманих з відкритих джерел. Так, розглядаючи клопотання прокурора про закриття кримінального провадження у зв'язку зі смертю обвинуваченого, було зазначено: «суд вважає, що у зв'язку з тимчасовою окупацією м. Сватово Луганської обл. неможливо зареєструвати смерть ОСОБА_3 в органах РАГС і в даному випадку можливо на підтвердження смерті ОСОБА_3 прийняти ті відомості, які зазначені прокурором за посиланням ІНФОРМАЦІЯ_5, як інформацію з відкритих джерел (OSINT)» [10]. В даному випадку слід звернути увагу, що доля всього кримінального провадження була вирішена виключно на відомостях, отриманих з відкритих джерел («в ході моніторингу мережі ІНТЕРНЕТ та зокрема, месенджеру TELEGRAM оглянуто телеграм канал під назвою «ІНФОРМАЦІЯ_3» (мовою оригіналу «ІНФОРМАЦІЯ_4» за посиланням ІНФОРМАЦІЯ_5. В ході огляду телеграм-каналу виявлена публікація за 18 березня 2024 року, згідно якої повідомляється про смерть депутата Адміністрації Сватівського муніципального округу ОСОБА_3»). Суд, розуміючи неможливість перевірити відомості у інший спосіб, прийняв рішення про закриття кримінального провадження.

В цілому можна помітити, що на даний момент судді все ще не ставлять суворих вимог щодо допустимості доказів, отриманих за допомогою OSINT. Проте, з урахуванням універсальності кримінального процесуального законодавства, а також через відсутність диференціації доказів, всі відомості мають оцінюватись з точки зору належності та допустимості. Дійсно, з урахування специфіки самої сутності таких доказів, легкість їх збирання та відносну простоту у перевірці їх достовірності неправильним буде твердження, що по відношенню до таких доказів не повинні застосовуватись певні особливі умови чи правила. Проте безумовним правилом

оцінки навіть тих доказів, які були отримані за допомогою OSINT, має бути законність їх отримання, адже, відповідно до принципу презумпції невинуватості, обвинувачення не може гуртуватися на доказах, отриманих незаконним шляхом.

В цілому, оцінюючи специфіку доказування за допомогою OSINT у кримінальному провадженні, в першу чергу завжди необхідно звертати увагу на дотримання засад захисту персональних даних. Дійсно, OSINT-аналітики працюють з відомостями, які знаходяться у відкритому доступі, в той же час межа такого відкритого доступу інколи буває вкрай розмита. Відповідно, для того, щоб стверджувати, що відомості, отримані за допомогою OSINT, можна було використовувати в якості доказів у кримінальному провадженні, в першу чергу має бути доведено, що в процесі збирання таких доказів не було порушено засади ЗУ «Про доступ до публічної інформації» та інших суміжних нормативно-правових актів. Однак на практиці виникають і інші проблеми, які досі не мають вирішення з точки зору законності або незаконності отримання відомостей з відкритих джерел. В першу чергу це стосується офіційно заблокованих інтернет ресурсів.

Так, Указами Президента України №133/2017 від 15.05.2017 року та №227/2023 від 15.04.2023 року була введена низка обмежені відповідно до ЗУ «Про санкції», в тому числі заборона Інтернет-провайдерам надавати послуги з доступу користувачам мережі Інтернет до низки ресурсів (в тому числі і до окремих соціальних мереж). Очевидно, що такі санкції були запроваджені з метою мінімізації негативного впливу ворожої пропаганди на громадян та уникнення поширення неправдивої інформації у вітчизняному віртуальному просторі. Крім того, блокування сайтів також може відбуватися «в межах виконання розпоряджень НЦУ (Національного центру оперативно-технічного управління електронними комунікаційними мережами України), який функціонує при Держспецзв'язку. Його повноваження визначає постанова Кабінету міністрів України № 812 «Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану» [11].

Проблема полягає в тому, що дуже часто для розслідування воєнних злочинів, які вчиняються на території України, а також з метою виявлення фактів державної зради, переходу на бік ворога або колабораціонізму необхідно використовувати відомості, які містяться у заборонених, але відкритих інтернет джерелах (в першу чергу мова йде саме про заборонені соціальні мережі). У зв'язку з цим і виникає питання – чи законним є збирання таких доказів з використанням інструментів OSINT стороною обвинувачення?

В першу чергу необхідно зазначити, що рішення про блокування відповідних Інтернет-ресурсів покладається лише на провайдерів таких послуг. З юридичної точки зору такі обов'язки не покладаються на кінцевого користувача. Відповідно, цей самий кінцевий користувач (слідчий, прокурор або будь-яка інша фізична особа) може використати, наприклад, VPN (virtual private network – віртуальна приватна мережа) для того, щоб обійти таке блокування. Саме так і збираються відомості з відкритих джерел відносно осіб, які зареєстровані в соціальних мережах, які підпадають під санкції, і існує безліч прикладів, коли зібрані в такий спосіб докази вже активно використовуються у кримінальних провадженнях.

Інтернет-провайдер може лише виконати блокування онлайн ресурсу (що від нього вимагається), але технічно не може перешкоджати кінцевому користувачу використовувати VPN.

В такому випадку виникає інше питання: чи законним є використання VPN та чи передбачена відповідальність за відвідування заблокованих Інтернет-ресурсів? Прямої заборони на використання VPN в нормативно-правових актах наразі немає. Навіть якщо проаналізувати судові рішення, то там VPN сервіси розглядаються лише як інструмент доступу, але сам факт його використання склад кримінального чи іншого правопорушення не створює. Так, в одному з відносно типових вироків зазначено наступне: «у період з 01.08.2022 року по 13.05.2023 року ОСОБА_3, діючи в у мовах воєнного стану, у зв'язку із військовою агресією Російської Федерації проти України, перебуваючи за адресою проживання по АДРЕСА_1, із використанням власного мобільного терміналу марки «Redmi Note 11», s/n НОМЕР_1, з власного акаунта (ІНФОРМАЦІЯ_2 «ІНФОРМАЦІЯ_3» в соціально орієнтованому ресурсі мережі Інтернет «Однокласники», який є відкритий і до якого мають доступ всі користувачі зазначеного ресурсу мережі Інтернет, за умови використання сервісу VPN, із використанням спеціалізованого програмного забезпечення «VPN Master», здійснила обхід блокування, встановленого Указами Президента України №133/2017 від 15.05.2017 року та №227/2023 від 15.04.2023 року, Інтернет ресурсу «Однокласники» та поширила матеріали, у яких міститься виправдовування, визнання правомірною збройної агресії Російської Федерації проти України, розпочатої у 2014 році, а також глорифікація осіб, які здійснювали збройну агресію Російської Федерації проти України, розпочату у 2014 році» [12]. Тобто суд розглядає VPN виключно як один із інструментів, який було використано для вчинення кримінального правопорушення, передбаченого ч. 2 ст. 436-2 КК України, але не визначає це як порушення саме по собі. Крім того, не є незаконним (з точки зору суду) в даному випадку і використання Інтернет ресурсу, на який було накладено санкції, адже кримінальна відповідальність настає саме за вчинення незаконних дій на такому ресурсі.

Проблема може полягати в тому, що Інтернет-провайдер, укладаючи договір з кінцевим користувачем, може передбачити обов'язок останніх утримуватися від відвідування таких сайтів (навіть з використанням спеціального програмного забезпечення), що може ставити під сумнів законність отримання доказів за допомогою VPN з використанням інструментів OSINT. Це, звичайно, буде залежати від самого Інтернет-провайдера. В той же час маловірогідним є те, що провайдер буде вказувати такі деталі у договорі, адже фактичного контролю за виконанням такого зобов'язання він не має. Якщо переглянути типові договори надання електронних комунікаційних послуг, то найближчим в даному аспекті обов'язок, який покладається провайдером на користувача, є обов'язок «не допускати використання кінцевого обладнання та абонентських ліній для вчинення протиправних дій або дій, що загрожують інтересам національної безпеки, оборони та охорони правопорядку» [13; 14]. Дане положення є вкрай загальним і більше стосується вже дій особи на Інтернет-ресурсах, а не на особливостях доступу до них.

Висновки і перспективи подальших досліджень. Таким чином можна зробити висновок, що хоча сервіси VPN і допомагають обійти запобіжники та від-

відувати ресурси, які потрапили під санкції, власне факт використання таких сервісів не є порушенням з точки зору чинного нормативного регулювання. Відповідно, оперативний працівник, слідчий або прокурор в момент збирання інформації з відкритих джерел в першу чергу виступає як звичайний користувач мережі Інтернет, а тому на нього поширюються загальні умови та правила користування, про які йшла мова вище. Дійсно, в подальшому такі відомості можуть бути використані як докази у кримінальному провадженні, що власне і відрізняє звичайного користувача від OSINT аналітика в межах кримінального провадження, в той же час, як вже було неодноразово зазначено, використовуючи загальнодоступні інструменти та відвідуючи загальнодоступні Інтернет джерела, працівники правоохоронних органів діють не як представники держави, а як звичайні абоненти. У зв'язку з цим можна стверджувати, що використання в кримінальному процесуальному доказуванні відомостей, отриманих з заборонених сайтів з використанням VPN не може вважатися підставою для визнання таких доказів недопустимими, адже вони були зібрані без порушень норм чинного законодавства.

Література

1. Дикий О.В., Сидорчук В.В. Поняття OSINT та суміжні категорії. *Юридичний науковий електронний журнал*. 2024. № 9. С. 332–335.

2. Білобров А.В., Клімушин П.С. Використання технологій OSINT для отримання інформації. *Протидія кіберзлочинності та торгівлі людьми*: Збірник матеріалів Міжнародної науково-практичної конференції (м. Харків, 27 травня 2020 року). С. 135–137.

3. Яровой Т.С. OSINT як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. *Експерт: парадигми юридичних наук і державного управління*. 2019. № 4(6). С. 201–208.

4. Мартинюк С.О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал*. 2021, № 9. С. 332–334.

5. Минько О.В., Іохов О.Ю., Оленченко В.Т., Власов К.В. Використання технологій OSINT для отримання розвідувальної інформації. *Експерт: парадигми юридичних наук і державного управління*. 2019. № 4(6). С. 201–208.

6. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса: Видавництво «Юридика», 2024. 180 с.

7. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 29.07.2024, справа № 202/1636/24. URL: https://reyestr.court.gov.ua/Review/120649976

8. Ухвала слідчого судді Заводського районного суду міста Миколаєва від 30.10.2024, справа № 487/2085/24. URL: https://reyestr.court.gov.ua/Review/122674217

9. Вирок Івано-Франківського міського суду Івано-Франківської області від 05.12.2024, справа № 344/19008/24. URL: https://reyestr.court.gov.ua/Review/123535737

10. Ухвала Павлоградського міськрайонного суду Дніпропетровської області від 19.06.2024, справа № 185/2082/24. URL: https://reyestr.court.gov.ua/Review/120171416

11. Беловолченко Г. «Надійно заблокувати щось в інтернеті неможливо». Як в Україні блокуються російські ресурси й чому це зачіпає легальні сайти. *DOU*: вебсайт. URL: https://dou.ua/lenta/articles/blocking-websites/

12. Вирок Кіровського районного суду м. Кіровограда від 23.06.2024, справа № 404/4646/23. URL: https://reyestr.court.gov.ua/Review/111797018

13. Умови надання електронних комунікаційних послуг приватного акціонерного товариства «Київстар». *Київстар*: вебсайт. URL: https://cdn.kyivstar.ua/sites/default/files/about/umovi_nadannya_telecom_poslug.pdf

14. Умови і порядок надання телекомунікаційних послуг ТОВ «лайвселл». *Lifecell*: вебсайт. URL: www.lifecell.ua

Анотація

Торбас О. О. **Особливості доказування за допомогою OSINT у кримінальному процесі.** – Стаття.

В статті автор аналізує специфіку здійснення кримінального процесуального доказування за допомогою відомостей, отриманих з відкритих джерел. Автор зазначає, що оцінюючи специфіку доказування за допомогою OSINT у кримінальному провадженні, в першу чергу завжди необхідно звертати увагу на дотримання засад захисту персональних даних. Дійсно, OSINT-аналітики працюють з відомостями, які знаходяться у відкритому доступі, в той же час межа такого відкритого доступу інколи буває вкрай розмита. Відповідно, для того, щоб стверджувати, що відомості, отримані за допомогою OSINT, можна було використовувати в якості доказів у кримінальному провадженні, в першу чергу має бути доведено, що в процесі збирання таких доказів не було порушено засади ЗУ «Про доступ до публічної інформації» та інших суміжних нормативно-правових актів. Однак на практиці виникають і інші проблеми, які досі не мають вирішення з точки зору законності або незаконності отримання відомостей з відкритих джерел. В першу чергу це стосується офіційно заблокованих інтернет ресурсів.

Автор робить висновок, що хоча сервіси VPN і допомагають обійти запобіжники та відвідувати ресурси, які потрапили під санкції, власне факт використання таких сервісів не є порушенням з точки зору чинного нормативного регулювання. Відповідно, оперативний працівник, слідчий або прокурор в момент збирання інформації з відкритих джерел в першу чергу виступає як звичайний користувач мережі Інтернет, а тому на нього поширюються загальні умови та правила користування, про які йшла мова вище. Дійсно, в подальшому такі відомості можуть бути використані як докази у кримінальному провадженні, що власне і відрізняє звичайного користувача від OSINT аналітика в межах кримінального провадження, в той же час, як вже було неодноразово зазначено, використовуючи загальнодоступні інструменти та відвідуючи загальнодоступні Інтернет джерела, працівники правоохоронних органів діють не як представники держави, а як звичайні абоненти. У зв'язку з цим можна стверджувати, що використання в кримінальному процесуальному доказуванні відомостей, отриманих з заборонених сайтів з використанням VPN не може вважатися підставою для визнання таких доказів недопустимими, адже вони були зібрані без порушень норм чинного законодавства.

Ключові слова: кримінальний процес, кримінальне провадження, процесуальна діяльність, OSINT, докази, доказування, властивості доказів.

Summary

Torbas O. O. **Peculiarities of proving using OSINT in criminal proceedings.** – Article.

In the article, the author analyzes the specifics of criminal procedural evidence using information obtained from open sources. The author notes that when assessing the specifics of evidence using OSINT in criminal proceedings, it is first of all necessary to pay attention to compliance with the principles of personal data protection. Indeed, OSINT analysts work with information that is in the public domain, at the same time the boundary of such open access is sometimes extremely blurred. Accordingly, in order to argue that information obtained using OSINT could be used as evidence in criminal proceedings, it must first be proven that in the process of collecting such evidence, the principles of the Law of Ukraine "On Access to Public Information" and other related regulatory legal acts were not violated. However, in practice, other problems arise that still have no solution from the point of view of the legality or illegality of obtaining information from open sources. First of all, this applies to officially blocked Internet resources.

The author concludes that although VPN services help to bypass the safeguards and visit resources that have fallen under sanctions, the very fact of using such services is not a violation from the point of view of current regulatory regulations. Accordingly, an operational officer, investigator or prosecutor at the time of collecting information from open sources primarily acts as an ordinary Internet user, and therefore the general terms and conditions of use, which were discussed above, apply to him. Indeed, in the future, such information can be used as evidence in criminal proceedings, which actually distinguishes an ordinary user from an OSINT analyst within the framework of criminal proceedings, at the same time, as has been repeatedly noted, using publicly available tools and visiting publicly available Internet sources, law enforcement officers act not as representatives of the state, but as ordinary subscribers. In this regard, it can be argued that the use of information obtained from prohibited sites using VPN in criminal procedural evidence cannot be considered a basis for recognizing such evidence as inadmissible, since it was collected without violating the norms of current legislation.

Key words: criminal process, criminal proceedings, procedural activities, OSINT, evidence, proving, properties of evidence.