ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЦИФРОВИХ ДАНИХ OSINT У МІЖНАРОДНІЙ ПРАКТИЦІ

Латиш Катерина,
асистент кафедри криміналістики
Національного юридичного університету імені Ярослава Мудрого,
стипендіат MSCA4Ukraine, директор Центру українського права Вільнюського університету, кандидат юридичних наук, доцент

Науково-технічний прогрес стимулював появу нових видів та форм фіксації подій, а також розширення кола суб'єктів, які здійснюють таку фіксацію з подальшим розміщенням у Всесвітній мережі Інтернет. Дані з відкритих джерел почали використовувати щонайменше з часів Другої Світової війни, проте з тих часів значно змінилися технології збору даних, а також кількість людей, які володіють технічними засобами для такої фіксації, що вимагає концептуально іншого підходу для збору та подальшого аналізу зібраної інформації. Враховуючи кількість вже зареєстрованих воєнних злочинів на території України цілком зрозумілим є те, що українська справа може стати модельною для побудови належної та ефективної системи поводження з цифровими даними. Одним зі свідчень цього є також створення спеціальної окремої платформи[1] Офісом прокурора Міжнародного кримінального суду для збору таких цифрових даних від усіх без виключень суб'єктів, навіть анонімних. Тоді постає цілком закономірне питання щодо того, яким чином буде здійснюватися аналіз та оцінка такої інформації з огляду на значний обсяг матеріалу та обмеженість ресурсів Офісу прокурора Міжнародного кримінального суду. Можливим варіантом може бути використання штучного інтелекту, проте цей інструмент є не достатньо дослідженим та апробованим щодо таких випадків. Тому необхідно погодитися з тим, що широке впровадження у слідчу та судову практику даних з відкритих джерел потребує активізації розроблення та впровадження прогресивних технологій, які ґрунтуються на застосуванні сучасних криміналістичних знань, дотримуючись стандартів доказування у кримінальному провадженні та широкого застосування цифрових технологій і штучного інтелекту[2].

На широких можливостях по документуванню воєнних злочинів користувачами смартфонів, інших технічних засобів з функціями фото та відеофіксації, можливостях он-лайн трансляцій на мільйонну аудиторію акцентують увагу і науковці[3]. Кожен пересічний громадянин, який має у своєму розпорядженні смартфон з камерою може генерувати цифрову інформацію, навіть, використовуючи спеціальні безкоштовні додатки накшалт Eyewitness to Atrocities app[4], який зберігає метадані та інші важливі для подальшої верифікації

[1] OTP link. URL: https://otplink.icc-cpi.int (дата звернення: 19.09.2023).

[2] Шевчук В.М. Цифрова криміналістика: воєнні виклики сьогодення та нові завдання у сучасних умовах. *Правові виклики сучасності* : матеріали всеукраїнського круглого столу (м. Харків, 20 грудня 2022 р.). Харків: Державний біотехнологічний університет, 2022. С. 35-39.

[3] Дуфенюк О. М. Розслідування воєнних злочинів в Україні: виклики, стандарти, інновації. *Baltic Journal of Legal and Social Sciences*. 2022. №1. С. 54. DOI: 10.30525/2592-8813-2022-1-6 (дата звернення: 19.09.2023).

[4] Eyewitness to Atrocities app URL: https://www.eyewitness.global (дата звернення: 19.09.2023).

ідентифікаційні ознаки. Однак, таке розміщення на одній і тій самій платформі у соціальних мережах може здійснюватися з різним рівнем доступу: не лише у відкритому, але й в обмеженому (наприклад, для певної аудиторії з друзів, однокласників, колег тощо). Тому більш доцільною назвою для такого типу інформації вбачається «user-generated evidence», яке буде охоплювати, як інформацію з відкрити доступом, так і обмеженим.

Отже, з'явилася можливість дистанційного пошуку цінної для досудового розслідування інформації, навіть не маючи доступу до місця події, що є особливо важливим під час розслідування воєнних та інших злочинів. Проведення розслідування з фізичним доступом до території не є можливим на окупованих територіях або тих, що тільки-но були звільнені, через високий ризик мінування. Разом з тим, на таких територіях перебуває цивільне населення, яке за допомогою звичайного телефону може фіксувати події, які відбуваються з подальшим розміщенням у соціальних мережах або надсиланням у спеціальні телеграм-канали, чат-боти та інше.

Важливим є саме збереження цих даних разом з вихідними ідентифікаційними даними, геолокацією, часом для подальшої можливої верифікації цього відео. Особі, яка здійснювала подібну фото-, відео фіксацію неможливо вивезти такі дані з окупованих територій через суцільний контроль та перевірку, зокрема у так званих «фільтраційних таборах», через які громадяни вимушені проходити з метою виїзду з окупованих територій. Окрім допиту, здійснюється повний огляд телефону та інших технічних носіїв особи, навіть пошук видалених файлів, а також огляд сторінок у соціальних мережах. Файли з фіксацією пошкоджень та руйнувань власних домоволодінь або квартир примушують видаляти без можливості відновлення. Тому є важливим розроблення алгоритму дій для таких осіб не лише з фіксації, але й віддаленого безпечного збереження таких даних.

У зв'язку з тим, що такий тип можливих доказів з'явився відносно нещодавно, наукове обґрунтування, так само, як і правозастосовна практика є недостатньо розробленою. Фактично, «пальму першості» з надання значення OSINT-доказам взяли неурядові громадські організації, які почали здійснювати збір інформації про воєнні злочини з використанням даних саме з відкритих джерел. Проте виникають питання щодо релевантності такої інформації та процесуальних можливостей долучення такої інформації, адже такі особи не є учасниками кримінального провадження. До кола свідків також такі особи не можуть бути віднесені, адже вони не бачили на власні очі події, які відбувалися. Так само як і не можуть вони бути віднесені до спеціалістів, адже вони не володіють спеціальними знаннями у певній галузі у розумінні кримінального процесу.

Щодо перевірки релевантності наданих відеофайлів, то, окрім призначення відповідних судових експертиз, з урахуванням міжнародної судової практики, необхідним є встановлення особи, яка перебувала на місці події, задля подальшого надання нею показань у суді. Це, зокрема, пояснюється наявністю принципу безпосереднього дослідження доказів. Так, в одній зі справ Міжнародного кримінального суду у судовому рішенні зазначено, що прокурор

посилаючись на практику Міжнародного трибуналу щодо колишньої Югославії (ICTY) та Міжнародного трибуналу щодо Руанди (ICTR), вказав, що відео докази «говорять» самі за себе (Lubanga case, ICC)[5]. З цього твердження можна припустити, що відеофайли можуть виступати окремим джерелом без обов'язкового підтвердження показаннями свідка.

Одним з перших випадків, коли Міжнародний кримінальний суд все ж таки розглядав в якості доказу мобільні відеозаписи, які були розміщені у соціальній мережі Facebook та на основі цього видав ордер на арешт, була справа проти лівійського командувача високого рангу Аль-Верфаллі Махмуда за вбивство 33 людей[6]. Однак, остаточного вироку по цій справі ще немає, тому зарано робити висновки яким чином судді зможуть оцінити такі докази. Хоча в іншій справі проти ймовірного члена філії Аль-Каїди Ахмада Аль-Факі Аль-Махді суд розглядав не лише відеозаписи з соціальних мереж, але й супутникові знімки на підтвердження знищення об'єктів культурної спадщини у Тімбукту, Малі[7]. Проте особа визнала себе винним та автентичність цих доказів не оскаржувалася і не ставилася під сумнів.

Слід зазначити, що Офіс прокурора є більш лояльним до інформації з відкритих джерел, ніж Міжнародний кримінальний суд, адже у своїх обґрунтуваннях посилався на звіти, підготовленими авторитетними міжнародними неурядовими організаціями. Проте Міжнародний кримінальний суд стає дедалі критичнішим щодо надмірної довіри Офісу прокурора до таких звітів, які, на думку суддів, не мають достатньої доказової сили[8]. До прикладу в одній зі справ (Prosecutor v. Gbagbo[9]) було багато посилань на звіти неурядових організацій (громадських організацій), Організації Об'єднаних Націй та роздруківки новин з різних сайтів, переважна більшість яких була заснована на значній кількості анонімних чуток. При цьому не проводилися додаткові слідчі дії та не призначалися судові експертизи для підтвердження їх автентичності чи правдивості. Суд зазначив, що, хоча ці звіти та новини допомагають встановити контекст, «такі докази жодним чином не можуть бути представлені як результати повного та належного розслідування» [10].

Таким чином, проблема оцінки даних з Всесвітньої мережі Інтернет на цей час перебуває на етапі становлення та формування. Міжнародна практика визнає таку інформацію як доказ, але в якості підтвердження контексту вчинення

---

[5] Situation in the Democratic Republic of the Congo in the case of the Prosecutor v. Thomas Lubanga Dyilo. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2014_09844.PDF

[6] Situation in Libya in the case of the prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2017_05031.PDF

[7] Zarmsky, Sarah. 2021. "Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law." *Journal of International Criminal Justice* 19 (1): 213–25. **https://doi.org/10.1093/jicj/mqab048**.

[8] Freeman, Lindsay. 2020. "Prosecuting Atrocity Crimes with Open Source Evidence : Lessons from the International Criminal Court." In *Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, 1:48–67. Oxford, United Kingdom: Oxford University Press.

[9] Gbagbo and Blé Goudé Case. The Prosecutor v. Laurent Gbagbo and Charles Blé Goudé. ICC-02/11-01/15. URL: https://www.icc-cpi.int/cdi/gbagbo-goude

[10] Gbagbo and Blé Goudé Case. The Prosecutor v. Laurent Gbagbo and Charles Blé Goudé. ICC-02/11-01/15. URL: https://www.icc-cpi.int/cdi/gbagbo-goude

воєнних чи інших міжнародних злочинів. Тобто, суди поки що обережні в наданні оцінки таким доказам.

Список використаних джерел.

1. OTP link. URL: https://otplink.icc-cpi.int (дата звернення: 19.09.2023).
2. Шевчук В.М. Цифрова криміналістика: воєнні виклики сьогодення та нові завдання у сучасних умовах. *Правові виклики сучасності* : матеріали всеукраїнського круглого столу (м. Харків, 20 грудня 2022 р.). Харків: Державний біотехнологічний університет, 2022. С. 35-39.
3. Дуфенюк О. М. Розслідування воєнних злочинів в Україні: виклики, стандарти, інновації. *Baltic Journal of Legal and Social Sciences*. 2022. №1. С. 54. DOI: 10.30525/2592-8813-2022-1-6 (дата звернення: 19.09.2023).
4. Eyewitness to Atrocities app URL: https://www.eyewitness.global (дата звернення: 19.09.2023).
5. Situation in the Democratic Republic of the Congo in the case of the Prosecutor v. Thomas Lubanga Dyilo. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2014_09844.PDF
6. Situation in Libya in the case of the prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2017_05031.PDF
7. Zarmsky, Sarah. 2021. “Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law.” *Journal of International Criminal Justice* 19 (1): 213–25. https://doi.org/10.1093/jicj/mqab048.
8. Freeman, Lindsay. 2020. “Prosecuting Atrocity Crimes with Open Source Evidence : Lessons from the International Criminal Court.” In *Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, 1:48–67. Oxford, United Kingdom: Oxford University Press.
9. Gbagbo and Blé Goudé Case. The Prosecutor v. Laurent Gbagbo and Charles Blé Goudé. ICC-02/11-01/15. URL: https://www.icc-cpi.int/cdi/gbagbo-goude
10. Gbagbo and Blé Goudé Case. The Prosecutor v. Laurent Gbagbo and Charles Blé Goudé. ICC-02/11-01/15. URL: https://www.icc-cpi.int/cdi/gbagbo-goude