ВІДКРИТІ ЦИФРОВІ ДАНІ В АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ СЛІДЧОГО: ПРАВОВІ МЕЖІ ТА ГАРАНТІЇ ПРОПОРЦІЙНОГО ВИКОРИСТАННЯ

Юрій Олександрович ЛЕМЕШКО,

аспірант закладу вищої освіти
«Міжнародний університет бізнесу і права»

Цифровізація досудового розслідування істотно розширила коло відомостей, доступних слідчому без застосування процесуального примусу. Державні портали, соціальні мережі, онлайн-карти та цифрові архіви дають змогу встановлювати події, зв'язки й часові послідовності. Берклівський протокол визнає пізнавальну цінність відкритих цифрових джерел, однак пов'язує їх використання з плануванням, перевіркою походження, належним збереженням і безпечною роботою з даними [1]. Тому наукова проблема полягає у визначенні меж, за яких технічна доступність інформації не перетворюється на необмежене спостереження за особою.

Закон України «Про доступ до публічної інформації» закріплює відкритість публічної інформації та можливість повторного використання відкритих даних [2]. Закон України «Про захист персональних даних», зі свого боку, вимагає законної мети, адекватності й ненадмірності обробки [3]. Перший підхід забезпечує інформаційну відкритість, другий — захищає особу від неконтрольованого накопичення відомостей. Їх системне тлумачення свідчить: відкритість визначає спосіб доступу до джерела, але не легітимує будь-яке подальше профілювання, об'єднання чи зберігання даних.

Окремо оприлюднені записи можуть мати низьку інформаційну чутливість, проте після автоматизованого зіставлення розкривати місце проживання, коло контактів, погляди, звички або переміщення особи. Отже, вихідні відомості й утворений на їх основі профіль мають різну інтенсивність втручання у приватність. Правова оцінка повинна охоплювати не лише публічність елементів, а й масштаб збирання, характер поєднання, зміст похідного висновку, строк зберігання та коло його користувачів.

У справі Catt v. the United Kingdom Європейський суд з прав людини відмежував правомірність первинного збирання поліцією відомостей від пропорційності їх подальшого зберігання та наявності ефективних гарантій [4]. На відміну від формального підходу, за якого публічність інформації автоматично зменшує очікування приватності, Суд врахував мету бази, чутливість даних, тривалість їх утримання й реальну потребу. Для слідчої аналітики це означає, що законне спостереження за відкритою подією не створює безстрокового дозволу на включення всіх виявлених осіб до пошукового масиву.

О. Кабанов і Т. Олексіюк наголошують на розмежуванні відкритих та захищених даних публічного сектору, повторне використання яких потребує спеціальних умов [5]. Берклівський протокол, натомість, акцентує на методичній надійності: ідентифікації джерела, фіксації контексту та збереженні оригіналу [1]. Перший підхід визначає правовий режим, другий —

якість роботи з відомостями. Для слідчого вони мають застосовуватися сукупно, оскільки технічно достовірний результат може бути одержаний із порушенням правових меж, а правомірно доступний масив — втратити цінність через неналежну фіксацію.

Відкриті цифрові дані в аналітичній діяльності слідчого пропонується визначити як відомості, доступні невизначеному колу осіб без подолання юридично значущого контролю, що використовуються в конкретному кримінальному провадженні для формування та перевірки версій, виявлення інформаційних прогалин і підготовки процесуальних рішень. Таке визначення не ототожнює відкритість із відсутністю правового режиму та підкреслює допоміжний характер аналітичного результату: він орієнтує подальше доказування, але не замінює належно одержаних і перевірених фактичних даних.

Основною гарантією доцільно визнати принцип подвійної правової релевантності. Його перший компонент стосується правомірності первинного одержання: джерело має бути відкритим, а доступ — не пов'язаним з обходом обмежень або використанням чужих облікових даних. Другий компонент означає сумісність конкретної аналітичної операції з метою, обсягом і строком первинного доступу. Отже, слід перевіряти не тільки, чи можна було одержати файл, а й чи допустимо саме так поєднувати, профілювати, зберігати та передавати його зміст.

Для реалізації цього принципу пропонується матриця правомірності аналітичного використання. Вона має відображати джерело, дату й спосіб доступу, категорії даних, зв'язок із конкретною версією, заплановані операції, часові межі, ризик утворення чутливого висновку, строк зберігання та умови припинення використання. Матриця не дублює процесуальний документ, а фіксує відповідність між інформаційною потребою і масштабом пошуку до включення відомостей у робочий масив.

Матрицю слід доповнити правилом незбільшення втручання за замовчуванням. Технічна логіка заохочує розширювати масив, тоді як правова вимагає починати з найменшого обсягу, достатнього для перевірки версії. Додавання нових категорій осіб, збільшення часового інтервалу або підключення геолокаційних чи біометричних параметрів має ґрунтуватися на окремо задокументованій інформаційній прогалині. Це конкретизує вимоги адекватності й ненадмірності обробки персональних даних [3].

Якщо завдання можна розв'язати адресним запитом або фільтрацією за обмеженим періодом, повне копіювання відкритого реєстру є надмірним. Доцільною є модель контрольованого аналітичного опрацювання: пошукові операції виконуються на стороні володільця або в захищеному середовищі, а слідчий одержує релевантний результат і мінімальні метадані для перевірки [5]. Фіксацію слід забезпечити паспортом відкритого цифрового джерела, який містить ідентифікатор, дату й час отримання, програмний засіб, контрольну суму за можливості, опис контексту, виконані перетворення та місце зберігання оригіналу [1].

Правомірність повинна перевірятися протягом усього життєвого циклу даних. Відповідно до підходу у справі Catt v. the United Kingdom відсутність строків перегляду може зробити непропорційним навіть первинно

виправдане збирання [4]. Робочі масиви слід переглядати після спростування версії, зміни статусу особи, закриття провадження або втрати зв'язку з предметом доказування. Відомості про непричетних осіб мають відокремлюватися, знеособлюватися чи видалятися, якщо закон не вимагає їх зберігати.

Принциповим залишається розмежування аналітичного орієнтира та процесуального доказу. Інформація з відкритого джерела може бути підставою для побудови версії, визначення особи для перевірки або підготовки клопотання про проведення процесуальної дії. Проте висновок про причетність не повинен ґрунтуватися лише на автоматизованому збігу, мережевому профілі чи непідтвердженому цифровому матеріалі. Методичну перевірку джерела необхідно доповнювати процесуальним підтвердженням тих первинних фактів, які надалі використовуються у доказуванні. Це зберігає оперативність відкритої аналітики, але не допускає підміни визначеної законом процедури технологічно переконливим припущенням.

Організаційна модель контролю має розмежовувати функції ініціатора, виконавця та контролера. Слідчий визначає мету і зв'язок завдання з кримінальним провадженням; аналітик виконує пошук та документує критерії; уповноважена посадова особа перевіряє масиви підвищеного ризику, строки зберігання й розширення початкового завдання. На відомчому рівні доцільно затвердити форми матриці правомірності та паспорта джерела, правила мінімізації робочого масиву і періодичність його перегляду. Аналітичне поєднання законно одержаних даних не повинно створювати самостійної підстави для доступу до інших джерел, а рішення про наступний процесуальний захід має залишатися персоніфікованим, мотивованим і перевірюваним.

Контроль не повинен обмежуватися перевіркою після скарги або витоку. Автоматизовані журнали доступу доцільно використовувати для виявлення нетипово великих запитів, повторного пошуку щодо непричетних осіб і звернень поза визначеним періодом. Виявлення індикатора не доводить порушення, але має ініціювати документовану перевірку мети, правової підстави та обсягу операції. Ефективність розслідування не може компенсувати невизначену підставу доступу, надмірний масив або порушення строку зберігання.

Отже відкритість цифрового джерела характеризує спосіб доступу, а не надає універсального дозволу на необмежене збирання, агрегування та зберігання даних. Правомірність їх використання слід визначати за метою, обсягом, способом опрацювання, чутливістю похідного висновку, строком зберігання й перевірюваністю. Запропоновані принцип подвійної правової релевантності, правило незбільшення втручання, матриця правомірності та паспорт відкритого цифрового джерела поєднують оперативність аналітики з вимогами законності, пропорційності й мінімізації даних.

Список використаних джерел:

1. Office of the United Nations High Commissioner for Human Rights; Human Rights Center, University of California, Berkeley, School of Law. Berkeley Protocol on Digital and Open Source Investigations. New York ; Geneva : United Nations, 2022. URL: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source.

2. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/go/2939-17.

3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17.

4. European Court of Human Rights. Case of Catt v. the United Kingdom, application no. 43514/15, judgment of 24 January 2019. URL: https://hudoc.echr.coe.int/eng?i=001-189424.

5. Кабанов О., Олексіюк Т. Відповідність законодавства України окремим положенням правового регулювання сфери відкритих даних у Європейському Союзі : аналітичний звіт. Київ : Міністерство цифрової трансформації України, 2023. URL: https://eef.org.ua/wp-content/uploads/2023/07/Vidpovidnist-zakonodavstva-Ukrayiny-okremym-polozhennyam-pravovogo-regulyuvannya-sfery-vidkrytyh-danyh-u-YEvropejskomu-Soyuzi.pdf.