Проблеми фіксації цифрової інформації в кримінальному провадженні

Галина Авдєєва

Канд. юрид. наук, НДІ вивчення проблем злочинності НАПрН України, м. Харків, Україна,
ORCID: https://orcid.org/0000-0003-4712-728x, e-mail: gkavdeeva@gmail.com

Продемонстровано помилки у фіксації цифрової інформації співробітниками правоохоронних органів. Запропоновано в програму підготовки співробітників правоохоронних органів додати дисципліну щодо роботи з цифровими доказами.

Ключові слова: цифрова інформація; цифровий доказ; фіксація цифрової інформації; кримінальне провадження.

Problems of Recording Digital Information in Criminal Proceedings

Galina Avdeeva

The paper demonstrates errors in recording digital information by law enforcement officers. It is proposed to incorporate discipline on handling digital evidence into the law enforcement officers' training program.

Keywords: digital information; digital evidence; digital information recording; criminal proceedings.

Завдяки розвитку сучасних технологій цифрова інформація стає дедалі вагомішою у розслідуванні злочинів. Нею слугують цифрові відеозаписи, дані з комп'ютерів, мобільних пристроїв, соціальних мереж, електронної пошти, вебсайтів, баз даних та ін.

В Україні зокрема функціонують кілька платформ для фіксування злочинів, скоєних російськими військовими, одна з провідних поміж них — Українська Гельсінська Спілка з прав людини. У лютому 2024 р. загальна кількість злочинів склала 45 204 від початку повномасштабного вторгнення. Значна частина задокументованих воєнних злочинів (13 428) пов'язана з людськими втратами або порушеннями прав цивільного населення [1]. Однак, на сьогодні суди в Україні ухвалили лише 80 вироків щодо воєнних злочинців. У судах перебувають 350 справ, в яких 512 підозрюваних вдалося ідентифікувати [2]. На жаль, накопичену в базах даних цифрова інформація не завжди можна використати як доказ у кримінальному провадженні. Вона може слугувати джерелом доказів під час розслідування злочинів лише за умови її відповідності критеріям оцінки доказів (допустимість, належність, достовірність і достатність).

Допустимість доказу визначається законністю джерела походження та способу отримання. Належність віддзеркалює здатність доказу підтверджувати або спростовувати будь-які обставини, що мають значення для справи. Достатнім є доказ, який віддзеркалює його здатність підтверджувати або спростовувати обставини, що мають значення для справи. Доказ вважають достовірним, якщо він відповідає дійсності [3].

Л. Лобойко стверджує, що значення терміну «достовірність» у кримінальному процесі та у точних науках відрізняється. У точних науках — це рівна одиниці ймовірність, а в кримінальному процесі — «*так звана практична достовірність, якою переважна більшість людей, які перебувають у здоровому глузді, задовольняється в найбільш відповідальних ситуаціях повсякденного життя*» [4, с. 187]. Суд може визначити достовірність цифрових доказів за допомогою протоколів процесуальних дій, під час проведення яких фіксували цифрову інформацію, або за показаннями свідків (зокрема, ними можуть бути співробітники правоохоронних органів, які вилучали електронні пристрої або фіксували (копіювали) інформацію в цифровій формі).

Кримінальний процесуальний кодекс України не містить положень про електронні (цифрові) докази та порядок їх фіксації. Неякісна та неповна фіксація цифрової інформації в подальшому може призвести до невизнання її джерелом доказів у кримінальному провадженні.

Міжнародна організація *Global Rights Compliance* оприлюднила «Керівництво з базових стандартів розслідування для

© Г. Авдєєва, 2024

документування міжнародних злочинів в Україні» [5], в якому особливу увагу приділено використанню цифрової інформації у розслідуванні воєнних злочинів. У керівництві надано інформацію про основні правила розслідування, підготовку до документування та роботи з різними видами доказів (фізичними, документальними, цифровими, аудіовізуальними та інформацією з відкритих джерел). У виданні наведено докладний порядок фіксації інформації у цифровому вигляді.

П. Левуліс після узагальнення 370 завершених кримінальних проваджень з використанням цифрових доказів визначив, що лише у 19 випадках для дослідження цифрових доказів залучали судових експертів, в інших провадженнях суди оцінювали їх самостійно шляхом дослідження роздруківок, наданих до суду сторонами у справі. У 84 провадженнях суд визнав автентичність (справжність) змісту роздруківок без використання спеціальних знань. Підтвердженням автентичності роздруківок цифрових доказів слугували засвідчення їх нотаріусом, підписом особи, яка їх надавала суду, отримання офіційної довідки від працівника поліції, який виконував роздруківку, або показань свідків, які підтверджували їх автентичність. У жодному з 370 випадків правоохоронці не забезпечили фіксацію цифрових доказів безпосередньо шляхом виготовлення перевіреної цифрової копії. Вони зазвичай обмежувались протоколюванням та роздруківками, а вилучені електронні пристрої зазвичай не були описані в протоколах достатньо, щоб їх могли ідентифіковати в майбутньому (35 із 62 вилучених пристроїв були описані лише із зазначенням марки та кольору пристрою) [6]. Таке узагальнення свідчить про недостатній рівень обізнаності співробітників правозастосовних органів щодо роботи з цифровими доказами та важливість належної фіксації цифрових доказів.

Науковці у галузі кримінально-правових наук наголошують на низькому рівні підготовки слідчих до роботи із програмно-технічними комплексами та складними програмними оболонками. Тому вони вважають, що залучення спеціаліста під час роботи з цифровими доказами є обов'язковим, оскільки найменша некваліфікована дія може призвести до втрати важливої доказової або орієнтувальної інформації [7, с. 135].

Поліцейські академії США задля попередження слідчих помилок під час роботи з цифровими доказами в програму підготовки (перепідготовки) співробітників поліції додали дисципліну щодо роботи з цифровими доказами на основі відповідних настанов [8]. Розробники цих програм зазначають, що цифрові докази можуть бути марними без визначення їхньої достовірності та докладної фіксації ланцюжка зберігання доказів. Вони розробили алгоритми протоколювання процесуальних дій із використанням цифрових доказів і зазначили перелік питань, які мають бути висвітлені в протоколах [9].

Науковці Національного інституту юстиції США зазначають важливість докладного протоколювання процесів автентифікації (визначення справжності) та решти дій із цифровими доказами (вилучення з докладним описом електронного пристрою; зазначенням його власника та осіб, які мали до нього доступ; способів і засобів вилучення інформації; копіювання на зовнішній носій; дослідження з описом методів і засобів тощо), що дає змогу довести факт зберігання інформації у первісному вигляді [10, с. 13].

У співробітників правозастосовних органів під час виявлення, фіксування, зберігання та оцінювання доказової інформації у цифровому вигляді виникають певні труднощі через складність і різноманітність знань, необхідних для виконання таких дій.

Особливої актуальності під час розслідування воєнних злочинів набули проблеми фіксації цифрової інформації, коли безліч цифрової інформації про воєнні злочини і воєнних злочинців накопичена в різних базах даних, а суд може не визнати її процесуальним джерелом доказів через неякісну фіксацію. Тому програми підготовки та підвищення кваліфікації співробітників правозастосовних органів слід доповнити базовою підготовкою щодо роботи з цифровими доказами.

Перелік джерел посилання

1. Задокументовані воєнні злочини у лютому 2024 року: огляд / Українська Гельсінська Спілка з прав людини. 18.03.2024. URL: https://www.helsinki.org.ua/articles/zadokumentovani-voienni-zlochyny-vprodovzh-sichnia-2024-ohliad/ (дата звернення: 19.03.2024).

2. Губа Р. Костін: Суди ухвалили 80 вироків щодо воєнних злочинів РФ / Deutsche Welle. 25.02.2024. URL: https://www.dw.com/uk/sudi-uhvalili-80-virokiv-sodo-voennih-zlocincivvijsk-rf-genprokuror/a-68369914?maca=ukr-rss-ukrnet-ukr-all-3816-xml (дата звернення: 17.03.2024).
3. Пільков К. М. Властивості доказів та критерії їх оцінювання. *Господарське право і процес.* 2020. № 4. С. 88—93. DOI: 10.32849/2663-5313/2020.4.14 (дата звернення: 19.03.2024).
4. Лобойко Л. М., Банчук О. А. Кримінальний процес : навч. посіб. Київ, 2014. 280 с.
5. Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні / Global Rights Compliance. Травень 2023. URL: http://surl.li/oomws (дата звернення: 18.03.2024).
6. Lewulis P. Digital forensic standards and digital evidence in Polish criminal proceedings. An updated definition of digital evidence in forensic science. *International Journal of Electronic Security and Digital Forensics.* 2021. No 13(4). Pp. 403. DOI: 10.1504/IJESDF.2021.10034988 (дата звернення: 19.03.2024).
7. Головкін Б. М., Денькович О. І., Луцик В. В., Цехан Д. М. Кіберзлочинність та електронні докази : навч. посіб. / за ред. О. Денькович, Г. Шмельцер. Львів, 2022. 298 с.
8. Hagy D. W. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors / U.S. Department of Justice. Office of Justice Programs. July 19, 2012. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors (дата звернення: 13.03.2024).
9. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors / U.S. Department of Justice. Office of Justice Programs. Jan, 2007. Pp. 15—17. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors (дата звернення: 19.03.2024).
10. Goodison S. E., Davis R. C., Jackson B. A.. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence : Research report. RAND Corp., 2015. 32 p. URL: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf (дата звернення: 17.03.2024).