DOI https://doi.org/10.30525/978-9934-26-685-0-9

# ЦИФРОВІ ДОКАЗИ У МІЖНАРОДНОМУ КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ ТА ПРОБЛЕМАХ З ПРАВАМИ ЛЮДИНИ

**Марченко А. Р.**

**ВСТУП**

Поява інтернету та поширення цифрових інструментів суттєво змінили соціальні практики. Переважна більшість населення має доступ до інтернету, а три чверті володіють принаймні одним підключеним мобільним телефоном. Водночас програми для обміну миттєвими повідомленнями та підключені пристрої постійно розвиваються. Правопорушники також скористалися цими технологічними розробками, що відзначилося масовим зростанням використання методів шифрування для зв'язку та цифрових медіа. Раніше шифрування було атрибутом організованої злочинності, а тепер стосується всіх користувачів. Нерозривно пов'язане з викриттями щодо американських програм перехоплення, шифрування стало ключовим аргументом продажу, який широко просувають оператори та виробники цифрових медіа. Шифрування, яке є важливим для дотримання основоположного права на приватність та для безпеки інформаційних систем, також є перешкодою для судових розслідувань, оскільки воно може виступати справжньою «стіною» для збору цифрових доказів.

Однак, «від розкриття кримінального правопорушення до суду над його винуватцем, вся система кримінального правосуддя обертається навколо вирішального питання доказів». Крім того, згідно з дослідженням, проведеним Європейським Союзом (ЄС), «понад 85% кримінальних розслідувань зараз вимагають збору цифрових даних». Дійсно, ці дані надають інформацію про особисте чи професійне життя підозрюваного чи жертви: історію дзвінків, обмін електронною поштою, повідомлення, електронні календарі, банківські операції, записи мобільних телефонів та геолокацію підключених пристроїв. Цифрові докази особливо різноманітні. Вони також вимагають певного рівня технічних знань. Часи, коли слідчі вимагали зізнань від головного(их) підозрюваного(их), давно минули. Цифрові докази – це, безсумнівно, технічні докази, засновані на використанні комп'ютерних інструментів, зокрема програмного забезпечення, яке іноді може бути складним в експлуатації. Таким чином, зростаючий інтерес до методів збору цифрових доказів пояснюється неадекватністю традиційних методів розслідування перед обличчям дедалі складніших та хитріших злочинів.

## 1. Цифрові докази у справах стосовно порушень прав людини та міжнародного кримінального правосуддя

У праві доказів міжнародних кримінальних трибуналів зазвичай посилаються на стандарти прав людини без подальших уточнень. Це викликає деякі питання щодо того, які права підпадають під це поняття, та їхнього

правового джерела. Право на приватність, як чітко показують наведені справи, є одним з першочергових питань, коли йдеться про цифрові докази, через те, що інформація часто збирається за допомогою засобів, які можуть втручатися в приватне життя відповідної особи. Міжнародні кримінальні трибунали, починаючи з Міжнародного кримінального трибуналу щодо колишньої Югославії, чітко заявили, що це право підпадає під поняття «стандарту прав людини» для цілей вирішення питання про допустимість.

Цифрові докази відіграють більш важливу роль, ніж будь-коли, у всіх судових провадженнях, що проводяться під керівництвом державного прокурора або слідчого судді. Дійсно, слідчі служби можуть використовувати різні цифрові інструменти для доведення скоєння правопорушення. Судові вилучення комп'ютерних даних, таємні розслідування, перехоплення комп'ютерних даних, доступ до збереженої кореспонденції, геолокація та перехоплення комунікацій – все це методи, які різною мірою дозволяють отримувати дані, що стосуються підозрюваного або його оточення.

Цифрові технології проникли в усі аспекти нашого життя в сучасному світі. Як наслідок, цифрова інформація та докази стають дедалі важливішими у сфері кримінального правосуддя. Від мобільних телефонів до комп'ютерних мереж, цифрові відбитки пальців людини можуть бути критично важливими для розслідування та судового переслідування у міжнародних кримінальних справах. Цифрова інформація та докази сприяють збереженню справедливого та неупередженого судочинства, а також допомагають у документуванні подій та встановленні фактів, які можуть бути недоступними або невидимими для традиційних методів розслідування[1].

Загалом, у світі визнається, що цифрова інформація та докази стали складнішими в результаті складного та дедалі складнішого технологічного ландшафту серед споживачів та компаній. Тому вплив хмарних обчислень та зростаюче поширення Інтернету створюють постійні виклики для аналітиків цифрової криміналістики . Найбільше вражає визнання багатьма авторами впливу людського фактору та схильності до людських помилок у сфері інформації та цифрових доказів[2]. Цифрова криміналістика є важливою для правоохоронних органів у сучасних кримінальних розслідуваннях, оскільки технології розвиваються в інструменти для незаконної діяльності та уникнення розкриття інформації. Для успішного кримінального переслідування в суді необхідний ланцюг зберігання, щоб забезпечити цілісність та автентичність доказів. Однак, оскільки цифрові докази є делікатними та мінливими, управління їх збереженням та збором є значними труднощами.

Судова практика міжнародних кримінальних трибуналів показує, що, особливо в останні роки, вони все частіше використовують цифрові технології для встановлення фактів. Як і передбачалося в передумові, фактично, цифрові докази в міжнародному кримінальному судочинстві дозволили трибуналам

[1] Prysiazhniuk I., 'Use of digital evidence in criminal process: some issues of right to privacy protection', Visegrad Journal on Human Rights, 5 (2023), 81-88 https://doi.org/10.61345/1339 7915.2023.5.11

[2] Reedy P., 'Digital Evidence Review 2016–2019', Forensic Science International: Synergy, 2 (2020) 489–520 https://doi.org/10.1016/j.fsisyn.2020.01.015

вирішити деякі проблеми, які зазвичай тягне за собою переслідування міжнародних злочинів. Окрім перешкод для збору доказів, згаданих вище, цифрові інструменти також добре пристосовані для вирішення специфічних особливостей міжнародних злочинів. Складність таких злочинів пояснюється тим, що вони не обмежуються одним діянням, а відбуваються як частина ширшого плану поведінки та вимагають доказів як контекстуальних, так і конкретних елементів[3].

У таких випадках аеро- та супутникові знімки, а також відеозаписи можуть бути фундаментальними для демонстрації існування масових та тяжких руйнувань або вбивств, переміщення людей або військ, а також спустошених районів. Наприклад, Міжнародний кримінальний трибунал з питань колишньої Югославії у справі Толіміра звернувся до супутникових знімків, наданих Прокурору американськими військовими, щоб довести наявність місць поховань та перепоховань, будівель та транспортних засобів, великих груп в'язнів та тіл у певних місцях. У справі Крстича аерофотознімки були використані для доведення масових та тяжких вбивств, скоєних у Сребрениці[4].

Приклади використання супутникових знімків як доказів фактів також можна знайти в практиці Міжнародного кримінального суду. Наприклад, у справах Дарфура Прокурор широко посилався на звіт Комісії з розслідування, призначеної для встановлення фактів, які мали місце під час насильницької кампанії уряду проти повстанців. Звіт, у свою чергу, здебільшого спирався на супутникові знімки, надані правозахисними організаціями, які використовували їх для виявлення руйнувань та спалень сіл, а також переміщення біженців[5]. У справі Аль-Махді прокурор представив значну кількість доказів з відкритих джерел, включаючи супутникові знімки, знайдені в Google Earth[6].

Хоча, як обговорюється нижче, використання такого роду зображень як доказів може створювати проблеми з їхньою надійністю, їх впровадження в судове провадження свідчить про поширеність інтернету та цифрових інструментів навіть у контексті судово-медичної експертизи. Ця тенденція продовжується у використанні сучасних технологій, і, зокрема, аеро- та супутникових знімків тіл на вулицях українських міст, для документування вбивств цивільного населення російською армією і, отже, для позначення скоєння воєнних злочинів.

У справі Благоєвича та Йокича перехоплені повідомлення були представлені прокурором Міжнародного кримінального трибуналу щодо колишньої Югославії як доказ «спілкування між офіцерами та солдатами Головного штабу ВРС, Дринського корпусу та підпорядкованих бригад протягом тижнів до, під час та після падіння Сребрениці… Дійсно, окремо розглянуті деякі перехоплення надають прямі докази того, що обвинувачений

[3] Dubber-ley, S.; Koenig, A.; Murray, D. (eds.), Digital Witness – Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, Oxford University Press, Oxford, 2019, pp. 48-67.

[4] Prosecutor v Radislav Krstic, Case No. IT-98-33, Judgement, 2 August 2001, respectively paras. 237 and 253.

[5] Report of the International Commission of Inquiry on Darfur to the United Nations Secretary-General, 2005, paras. 183 and 301, [https://www.legal-tools.org/doc/1480de/pdf/]

[6] Prosecutor v Al Mahdi, Case No. ICC-01/12-01/15-171

знав про насильницьке виселення цивільних мусульман зі Сребрениці та подальшу різанину мусульманських чоловіків у Сребрениці та/або брав у них участь. Можливо, що ще важливіше, в цілому перехоплені докази розповідають історію участі військових ВРС у нападі на Сребреницю та подіях, що настали, і є важливою частиною мозаїки доказів, які мають бути представлені обвинуваченням»[7].

МКС також посилався на перехоплені повідомлення. У справі Онгвен прокурор представив Палаті як доказ радіоперехоплення Армії опору Бога (ЛРА), перехоплені угандійськими службами безпеки. Зокрема, він подав Суду короткий зміст перехопленої інформації, який був підготовлений перехоплювачами після серії перехоплень і мав на меті транскрибувати та узагальнити англійською мовою зміст повідомлень (які переважно були мовами ачолі або луо, двома місцевими діалектами). Перехоплювачі передали записи з журналів своїм командирам, які передали перехоплені повідомлення до Кампали для інформування Народних сил оборони Уганди про ширші військові операції. Усі завершені записи та журнали реєстрації надійно зберігалися або в місцях перехоплення, або в Кампалі[8]. Те, що Прокурор подав Палаті, було результатом як відбору, здійсненого урядовими органами Уганди під час передачі записів та нотаток, зроблених перехоплювачами, так і процесу «покращення» аудіозаписів[9]. Щоб подолати сумніви та критику, що супроводжували подання перехоплених повідомлень, фундаментальну роль відіграли так звані «свідки перехоплення» – свідки, які могли обговорити операції перехоплення, а також конкретні перехоплені повідомлення. Свідків викликав Прокурор для дачі показань перед Судом з метою, по-перше, ідентифікації осіб, які говорили, та підтвердження відповідності аудіозаписів стенограмам, а по-друге, пояснення методології, яка використовувалася для покращення аудіо з метою кримінального провадження. Залишивши осторонь усі ці питання, які будуть детальніше обговорені нижче, варто зазначити, що перехоплені повідомлення були використані як доказ рангу Онгвена як командира бригади та його «взаємодії, зокрема з мережею радіозв'язку ЛРА, під час якої обговорювалися наміри завдати шкоди цивільному населенню через їхню передбачувану зв'язок з урядом Уганди. Крім того, Палата знаходить підтвердження для цього висновку у своїх висновках щодо участі Домініка Онгвена у чотирьох нападах, що стосуються звинувачень»[10].

Використання цифрової інформації та доказів досліджується відповідно до кількох міжнародних процесів та стандартів. По-перше, отримання цифрової інформації та доказів, щоб створити копію цифрових даних з певного джерела даних, що є важливим кроком у цифровому розслідуванні. Оскільки це

[7] Prosecutor v Blagojević and Jokić, Case No. IT-02-60-T

[8] Prosecutor v Dominic Ongwen, Case No. ICC-02/04-01/15, Judgment, 4 February 2021, para. 614 ff.

[9] Marchesi, D., Intercepted Communications in the Ongwen Case: Lessons to Learn on Documentary Evidence at the ICC, International Criminal Law Review, Vol. 22, No. 5-6, 2022, pp. 920-940.

[10] Freeman, L.; Vazquez Llorente, R., Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age, Journal of International Criminal Justice, Vol. 19, No. 1, 2021, pp. 163–188.

дозволяє додатково вивчити цифрову інформацію та докази, одночасно зменшуючи ризик втрати та маніпуляцій з цифровими даними[11]. Друге: вивчення цифрової інформації та доказів шляхом перетворення цифрових даних у відповідну форму, яку може прочитати пересічна людина, та регулювання даних навколо них, а також виявлення потенційної цифрової інформації та доказів[12]. Третє: Аналіз цифрової інформації та доказів таким чином, щоб аналіз цифрової інформації та доказів був пов'язаний з ідентифікацією та оцінкою потенційних джерел цифрових доказів як інформації. Докази та дані, що зберігаються або передаються у двосторонній формі та ідентифіковані в процесі аналізу цифрової інформації та доказів як такі, що мають відношення до розслідування[13]. Четверте: Підготовка звітів про цифрову інформацію та докази, щоб цей процес був невід'ємною частиною всієї роботи з цифрового розслідування та способу передачі цифрової інформації та доказів[14]. Тому слід задокументувати детальну інформацію про всі заходи та процедури, навколо яких проводилося цифрове розслідування. А також про всі враховані міркування та всі результати, отримані під час підготовки звіту під час цифрового кримінального розслідування.

Цифрові докази також порушують питання щодо фундаментального принципу кримінального процесу: справедливості доказів. Вимога справедливості доказів, яка була майже абсолютною умовою для здійснення прав захисту та, загалом, для проведення справедливого судового розгляду. Цей принцип згодом було змінено. Дійсно, «стратегія, яку використовує державна посадова особа для встановлення правопорушення або ідентифікації його винних, сама по собі не є порушенням принципу справедливості доказів». Таким чином, в принципі, стратегема, що застосовується органами державної влади для отримання доказів, є допустимою. Як виняток, така стратегема буде несправедливою, якщо вона призведе до порушення основного права або основоположної гарантії особи, щодо якої ведеться розслідування.

Збір цифрових доказів створює численні проблеми для кримінального процесу: його зв'язок з основоположними принципами та правами є складним. Розширення різних методів збору доказів має як наслідок послаблення основоположних принципів та прав. Тому стає дедалі важливішим модернізувати правила, що застосовуються до збору цифрових доказів, щоб, з одного боку, підтримувати та зміцнювати можливості слідчих служб, а з іншого боку, зберігати основоположні права. Це складне узгодження має ґрунтуватися

[11] Animesh Kumar Agrawal, Aman Sharma, Sumitra Ranjan Sinha, and Pallavi Khatri, 'Forensic of an Unrooted Mobile Device', International Journal of Electronic Security and Digital Forensics, 12.1 (2020), 118-137 https://doi.org/10.1504/ijesdf.2020.10025327

[12] Michael Kohn, Mariki M. Eloff, and Jan Eloff, 'Integrated digital forensic process model', Computers and Security, 38 (2013), 103–115 https://doi.org/10.1016/j.cose.2013.05.001

[13] Bruce Nikkel, 'NVM Express Drives and Digital Forensics', Digital Investigation, 16 (2016), 38–45 https://doi.org/10.1016/j.diin.2016.01.001

[14] Radina Stoykova, Stig Andersen, Katrin Franke, and Stefan Axelsson, 'Reliability Assessment of Digital Forensic Investigations in the Norwegian Police', Forensic Science International: Digital Investigation, 40 (2022), 1-13 https://doi.org/10.1016/j.fsidi.2022.301351

на методичному підході, щоб порівнювати та зважувати методи цифрового розслідування з основоположними правами[15].

Цей методичний підхід дедалі помітніший у різних рішеннях, винесених Судом ЄС щодо складного питання зберігання та доступу до даних про з'єднання. З часом, зіткнувшись із недоліками первинного та вторинного права ЄС, Суд ЄС розробив сукупність прецедентної практики, спрямованої на посилення захисту основоположних прав.

Згодом це було перенесено Касаційним судом Франції в кількох рішеннях, які визнали кілька правил французького кримінального процесу несумісними з законодавством ЄС. Однак з 2022 року жодних законодавчих змін щодо цих питань не було внесено, і фактично дійсність розслідувань залишається завдяки обмежувальному режиму недійсності, встановленому Касаційним судом[16]. Проте ця ситуація є незадовільною: вкрай важливо перебудувати систему збору цифрових доказів. З огляду на її особливо нав'язливий характер щодо основоположних прав, їх захист не може бути забезпечений системою, створеною суддями. Тому зусилля щодо реформування цієї системи повинні бути зосереджені, з одного боку, на гарантіях, що стосуються різних методів збору доказів, а з іншого боку, на органах, які дозволяють та контролюють виконання цих заходів.

Різні стандарти, що стосуються збору цифрових доказів, страждають від фрагментації в рамках Кримінально-процесуального кодексу, а їхня структура виглядає непрозорою та фрагментованою в міру розвитку законодавства та судової практики. Одним із шляхів реформування може бути створення загального права цифрових доказів у кримінальному процесі, структурованого навколо методології збору даних та гарантій, пов'язаних зі ступенем втручання в приватне життя та тривалістю слідчих заходів як порогом для судового втручання.

Те саме спостереження стосується нових методів збору цифрових доказів. Дійсно, він постійно розвивається, будучи тісно пов'язаним з технологічним прогресом. Окрім технічних досягнень, він спирається на величезні практичні можливості, що пропонуються новими методами та технологіями доказування. Слідчі стикаються з постійно зростаючими обсягами даних для аналізу. Зберігаючи ці дані на серверах або фізичних носіях, які необхідно аналізувати у все стисліші терміни, вони становлять величезний виклик для слідчих[17]. Тому ШІ може дати значну надію на сприяння розслідуванням. Його зростаюче використання слідчими ставить під сумнів його роль в управлінні цифровими доказами. Так само користувачі технологічних рішень поширюють дедалі більше вільно доступної інформації в Інтернеті. Соціальні мережі та онлайн-комунікації є справжньою золотою жилою для слідчих. Однак більш-менш масовий та потенційно автоматизований збір інформації, доступної з відкритих

[15] Benoît A.. La preuve numérique en procédure pénale : un système à (re)construire. Recueil Dalloz, 2023, p. 697.

[16] Cass. Crim., 12 juill. 2022, nos 21-83.710, 21-83.820, 21-84.096 et 20-86.652.

[17] Audibert M. L'extraction et l'exploitation des données contenues dans des supports numériques. Actualité juridique Pénal, 2023 p. 116.

джерел в Інтернеті, у контексті судових розслідувань створює численні труднощі[18].

На завершення, збір цифрових доказів – це динамічна галузь, притаманна технологічному та технічному розвитку, а також практиці користувачів, як потерпілих, так і підсудних. Але це динамічна галузь, яка потребує глибокого та безперечного реформування, навіть якщо її основи в кримінальному процесі є міцними та дозволяють шукати справедливий баланс між захистом основних прав та розслідуванням, ідентифікацією та переслідуванням винних. Взаємодія між позитивним правом та технологічним розвитком є складною та виходить за межі всіх юридичних дисциплін. Що стосується кримінального процесу, важливо, щоб він зберігав певну гнучкість та адаптивність перед обличчям технологічного, зокрема цифрового, розвитку.

За відсутності чітких правових положень судова практика іноді встановлює застосовний режим шляхом судового тлумачення, як ми спостерігали щодо доступу до даних про трафік та місцезнаходження. Тому необхідно посилити правовий нагляд за цими методами збору цифрових доказів, не вдаючись, однак, до необгрунтованого легалізму. Цифрові технології становлять реальний виклик для сучасного суспільства, оскільки кіберпростір був побудований та існує незалежно від державного контролю. Визначення методів контролю за цими заходами не може бути виключно національною справою. Тим не менш, ми повинні остерігатися процедурної революції, яка видається небажаною. Цифрові методи розслідування змінили спосіб проведення розслідувань, але «це процеси, які змінилися під впливом технологій, але чия функція залишається незмінною»[19]. За цих умов ми повинні поставити під сумнів фундаментальний принцип права доказів: чи є докази законними, чи вони переконливі?

Тому вкрай важливо реформувати та краще регулювати збір цифрових доказів у кримінальному провадженні в рамках комплексної реформи кримінальних розслідувань. Ця загальна реформа має бути здійснена за участю всіх зацікавлених сторін: слідчих, магістратів, експертів, а також техніків та спеціалістів з цифрових розслідувань, з метою зробити кримінальний процес більш зрозумілим для неспеціалістів у цифрових розслідуваннях та для широкої громадськості. «Написання законодавства ніколи не було легким просто тому, що це мистецтво дизайну, вміння осягати суть. Саме тому не можна нехтувати умовами, за яких проводиться ця діяльність»[20].

## 2. Технічні вразливості та зміна цифрових доказів

Сама природа цифрових даних робить їх особливо вразливими до різних форм змін – як випадкових, так і навмисних. На відміну від традиційних паперових документів, де зміни зазвичай залишають видимі сліди, цифрові зміни даних можуть бути практично непомітними без глибокої технічної експертизи.

[18] Cass. Crim., 30 avril 2024, n° 23-80.962

[19] Vergès É. La preuve numérique, entre continuité et changement de paradigme. Revue Justice Actualités, ENM, n° 1, 2019.

[20] Urvoas,Jean-Jacques. Libres réflexions sur l’écriture de la loi. Actualité juridique Pénal, 2023, p. 85.

Метадані – технічна інформація, що супроводжує цифрові файли (дати створення та зміни, ідентифікатори авторів, GPS-координати фотографій тощо), часто є критично важливим доказом. Однак ці метадані можна обробляти за допомогою відносно доступних інструментів. Наприклад, програмне забезпечення, таке як ExifTool, дозволяє змінювати EXIF-дані фотографій, таким чином змінюючи інформацію, яка може бути вирішальною у суперечці.

Фішингові атаки ілюструють ще одну серйозну вразливість. Зловмисник може видавати себе за людину та створювати шахрайський контент від її імені. У справі Sony Pictures 2014 року хакери скомпрометували системи компанії і змогли не лише отримати доступ до конфіденційних даних, а й змінювати та видаляти інформацію, що ускладнювало розрізнення автентичних і пошкоджених даних.

- Підробка часових позначок
- Зміна метаданих EXIF, IPTC або XMP
- Крадіжка цифрової особистості
- Модифікація системних журналів
- Тонкі пошкодження цифрових файлів

Ланцюжок зберігання цифрових доказів є серйозним технічним викликом. Кожна передача, копія або аналіз цифрових доказів можуть потенційно вплинути на їхню цілісність. Технічні стандарти, такі як ISO/IEC 27037:2012, надають рекомендації щодо ідентифікації, збору, придбання та збереження цифрових доказів, але їх суворе застосування залишається значним практичним викликом.

Поява технологій дипфейків і генеративного штучного інтелекту значно розширила можливості створення фальшивих візуальних та аудіоцифрових доказів. Ці технології дозволяють створювати гіперреалістичні відео або аудіозаписи, де люди вимовляють слова, яких ніколи не казали, або виконують дії, яких ніколи не робили.

Яскравим прикладом є справа Габонських воріт у 2018 році, коли сумніви щодо автентичності відео президента Алі Бонго спричинили політичну кризу. Нещодавно, у 2023 році, дипфейки з оголошенням президента Байдена про військову мобілізацію продемонстрували зростаючу складність цих технологій і їхній потенціал дестабілізувати.

Стикаючись із цими загрозами, розробляються методи виявлення, зокрема на аналізі візуальних невідповідностей, вивченні рухів обличчя або аналізі метаданих. Але ці контрзаходи ведуть постійну технологічну гонку з дедалі складнішими інструментами для створення підробок.

Зіткнувшись із внутрішніми вразливостями цифрових доказів, було розроблено різні технічні та процедурні методи для підвищення їхньої надійності та зниження спірності. Ці підходи мають на меті встановити дві основні характеристики: автентичність (докази дійсно походять з ймовірного джерела) та цілісність (докази не підроблялися з моменту їх створення).

Електронний підпис є одним із стовпів цифрової автентифікації. Базуючись на криптографічних системах з публічним/приватним ключем, він дозволяє з високою впевненістю приписати документ його автору. Регламент eIDAS розрізняє три рівні електронних підписів, причому кваліфікований підпис

забезпечує найвищі юридичні гарантії, еквівалентні рукописному підпису. Касаційний суд підтвердив цей підхід у рішенні від 6 квітня 2016 року, визнавши доказову цінність кваліфікованого електронного підпису.

Сертифіковані електронні часові мітки є ще одним фундаментальним способом забезпечення цифрових доказів. Це дає змогу надійно підтвердити, що певний фрагмент даних існував у певний час. Сертифікаційні органи, такі як Universign або Certigna, видають сертифікати з часовими позначками, які відповідають міжнародним технічним стандартам, створюючи таким чином сильну презумпцію щодо дати існування цифрового документа.

Криптографічні хеш-функції (такі як SHA-256 або SHA-3) використовуються для створення унікального відбитка великого пальця файлу. Найменша зміна файлу, навіть на один біт, призведе до зовсім іншого відбитка пальця. Ця властивість використовується для перевірки цілісності цифрового документа шляхом порівняння його поточного відбитка з тим, що був розрахований при створенні.

Зіткнувшись із викликами, які виникають через оскаржливість цифрових доказів, стає надзвичайно важливим посилити загальну стійкість нашої системи доказів. Цей підхід передбачає скоординовані дії на кількох рівнях: технічному, юридичному, освітньому та інституційному.

Впровадження адаптивного управління технічними стандартами є першим важелем дій. Замість того, щоб заморожувати технічні стандарти, які швидко стають застарілими в законодавчих текстах, було б розумно застосувати більш гнучкий підхід, де закон визначає основні принципи, а спеціалізовані органи, такі як ANSSI або AFNOR, встановлюють і регулярно оновлюють технічні стандарти. Цей підхід був рекомендований Державною радою у її щорічному дослідженні 2017 року щодо державних органів влади та цифрових платформ.

Розвиток культури цифрових доказів – ще один важливий напрямок. Підвищення обізнаності громадян, компаній і адміністрацій про найкращі практики зберігання та захисту даних із доказовою цінністю дозволило б запобігти багатьом суперечкам заздалегідь. Ініціативи, такі як Паспорт цифрової економіки, можуть включати конкретний компонент управління електронними відкриттями у професійному чи особистому контексті.

Створення незалежних цифрових, довірених третіх сторін – це перспективний шлях для підвищення надійності електронних доказів. Ці суб'єкти, підпорядковані суворим зобов'язанням щодо нейтральності та прозорості, можуть відігравати посередницьку роль у сертифікації, збереженні та поверненні цифрових доказів. Модель традиційних міністерських офіцерів (нотаріусів, судових виконавців) може надихнути на появу цих нових гравців у цифровому трасті.

## 3. Електронні (цифрові) докази у кримінальному процесі України

В.М. Фігурський визначив такі ознаки електронних доказів:

1) їх творцем є як людина, так і комп'ютерна система;

2) мають нематеріальний вираз, що дає їм можливість зберігатися на відповідному носії (приміром смарт-годиннику, смартфоні, планшеті, ноутбуці, жорстких дисках, флеш-накопичувачах) чи кількох носіях одночасно, проте без

нероздільного зв'язку з ними або перебувати у цифровому середовищі (зокрема хмарному сховищі) без такого носія;

3) внаслідок цього підлягають сприйняттю лише завдяки використанню спеціальних тех нічних засобів і програмного забезпечення;

4) можуть зберігатися без змін упродовж тривалого часу, бути скопійовані чи переслані, не зазнаючи коригування їх змісту, та не мають обмежень у кількості разів використання;

5) з іншого боку, через свою природу докази в електронній формі піддатливі до маніпуляцій та знищення;

6) копії деяких доказів в електронній формі (документів) за наявності обов'язкових реквізитів (зокрема електронного підпису) прирівнюються до оригіна лу та можуть використовуватися у кількох справах одночасно[21].

Електронні документи мають свої особливості і до них висуваються певні вимоги, зокрема, це можуть бути текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо; вони зберігаються на картах пам'яті чи мобільних телефонах, на серверах чи системах ре зервного копіювання, а також на інших місцях збереження даних в електронній формі, в тому чис лі в мережі Інтернет; інформація в електронному документі зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, зокрема, електронний цифровий підпис[22].

Рекомендації щодо використання доказів в електронній формі у національних правових системах сформулювані й Комітетом Міністрів Ради Європи. Серед цих рекомендацій привертають увагу такі. Вирішувати потенційну доказову силу електронних доказів відповідно до національного законодавства мають суди. Електронні докази повинні оцінюватися так само, як і інші види доказів, зокрема щодо їх допустимості, автентичності, точності та цілісності. Обробка електронних доказів не повинна бути невигідною для сторін або надавати несправедливу вигоду одній із них. У принципі, суди не повинні заперечувати юридичну силу електронних доказів лише через відсутність вдосконаленого, кваліфікова-ного або аналогічного захищеного електронного підпису. Суди повинні знати про доказову силу метада-них і потенційні наслідки їх невикористання. Сторонам має бутидозволено подавати електронні докази в оригінальному електронному форматі без необхідності надання роздруківок. Беручи до уваги вищий ризик потенційного знищення або втрати електронних доказів порівняно з неелектронними доказами, держави-члени повинні встановити процедури безпечного вилучення та збору електронних доказів. Суди повинні знати про конкретні проблеми, які виникають під час вилучення та збору електронних доказів за кордоном, у тому числі в транскордонних справах. Електронні докази слід збирати, структу-рувати та управляти у спосіб, аби полегшити їх передачу до інших судів, зокрема до апеляційного суду. Слід заохочувати та сприяти передачі електронних доказів електронними засобами з

[21] Фігурський В.М. Докази в електронній формі у кримінальному провадженні. Галицькі студії. Юридичні науки. № 4, 2023. С. 97–105.

[22] Мілімко Л.В., Жидовцев Я.В. Електронні докази в кримінальному судочинстві України. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. Випуск 88: частина 3 С. 302-308

метою підвищення ефективності судового розгляду[23]. Системи та пристрої, що використовуються для передачі електронних доказів, повинні бути здатними зберігати їх цілісність. Суди можуть вимагати дослідження електрон-них доказів експертами, особливо коли порушуються складні доказові питання або якщо є підозри про маніпулювання електронними доказами. Суди повинні вирішувати, чи мають такі особи достатній досвід у цій справі. Що стосується достовірності, суди повинні враховувати всі відповідні чинники джерела та автентичності електронних доказів. Наскільки це дозволяє національна правова система та на розсуд суду, електронні дані повинні прийматися як докази, якщо достовірність таких даних не оспорюється однією зі сторін. Наскільки це дозволяє національна правова система та на розсуд суду, слід презюмувати достовірність електронних даних за умови, що особу підписанта можна підтвердити, а цілісність даних захищено, якщо і доки не буде є обґрунтовані сумніви в протилежному. Наскільки це передбачає національна правова система, якщо державний орган передає електронні докази незалежно від сторін, такі докази є переконливими щодо їх змісту, якщо і доки не буде доведено протилежне. Електронні докази слід зберігати таким чином, щоб зберігали читабельність, доступність, цілісність, автентичність, достовірність і, де це можливо, конфіденційність і приватність.

Електронні докази слід зберігати зі стандартизованими метаданими, щоб контекст їх створення був зрозумілим. Суди повинні архівувати електронні докази відповідно до національного законодавства. Електронні архіви повинні відповідати всім вимогам безпеки та гарантувати цілісність, автентичність, конфіденційність і якість даних, а також повагу до приватного життя. Судді та юристи-практики повинні знати про еволюцію інформаційних технологій, яка може вплинути на доступність та цінність електронних доказів. Правова освіта повинна включати модулі з електронних доказів[24].

## ВИСНОВКИ

Очікується, що право на цифрові докази буде швидко еволюціонувати, щоб адаптуватися до технологічних інновацій. Зростання Інтернету збільшить потенційні джерела електронних доказів. Голосові асистенти, підключені автомобілі та підключені об’єкти в будинку можуть стати мовчазними свідками у завтрашніх судових справах.

Блокчейн може революціонізувати управління цифровими доказами, забезпечуючи їх цілісність і відстежуваність. Ця технологія відкриває перспективні перспективи для забезпечення ланцюга зберігання електронних доказів і підвищення їхньої доказової цінності в суді.

Нарешті, поява штучного інтелекту в юридичній сфері породжує нові питання. Як оцінити надійність алгоритмічно згенерованого доказу? Яку цінність слід надавати прогнозній аналітиці на основі масової обробки судових

[23] Фігурський В.М. Докази в електронній формі у кримінальному провадженні. Галицькі студії. Юридичні науки. № 4, 2023. С. 97–105.

[24] Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings. Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers’ Deputies. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c

даних? Ці питання вимагають глибокого осмислення етичної та правової основи цих нових технологій.

Право на цифрові докази заявляє про себе як невід'ємний стовп сучасного правосуддя. Її розвиток вимагає постійної адаптації правової бази, технічних навичок і судових практик. Забезпечення справедливих судових процесів у повністю цифрову епоху є серйозним викликом для наших суспільств, що вимагає тісної співпраці між юристами, техніками та політичними керівниками.

**АНОТАЦІЯ**

Цифрова інформація та докази є складною галуззю на національному та міжнародному рівнях. Тому сучасні технології, що розвиваються з високою швидкістю, ускладнюють питання моніторингу інформації та цифрових доказів. Крім того, злочинці використовують кілька сучасних та передових тактик для приховування своєї злочинної діяльності, яка порушує права людини та міжнародне кримінальне право. Це ускладнює виявлення цифрової інформації та доказів під час скоєння міжнародних злочинів. У деяких практичних випадках, що вимагає розшифрування цих доказів, експертам стає складніше збирати та враховувати цифрову інформацію та докази.

З безперервним технічним та технологічним розвитком країн світу, держави мають можливість широко використовувати цифрову інформацію та докази. Переслідування державних злочинів є однією з тих сфер, де інформація та цифрові докази можуть бути використані для розслідування порушень прав людини та міжнародного кримінального права. Стало можливим покладатися на докази та інформацію, отриману через Інтернет, соціальні мережі або супутники. Це призводить до відстеження злочинців та підозрюваних, документування воєнних злочинів, злочинів проти людяності та геноциду. Таким чином, багато даних зберігаються в цифровому просторі, що призводить до появи нових видів кримінальних злочинів, пов'язаних з порушеннями прав людини та міжнародного кримінального права. Тому Інтернет, соціальні мережі та супутники широко використовуються у сфері спостереження за незаконною діяльністю, надаючи космічні знімки високої роздільної здатності районів, де відбуваються порушення прав людини та міжнародного кримінального права, фіксуючи такі дані та документацію та виявляючи підозрілу діяльність.

**Ключові слова:** цифрові докази, кримінальне судочинство, порушення прав людини, міжнародні стандарти

## Література:

1. Animesh Kumar Agrawal, Aman Sharma, Sumitra Ranjan Sinha, and Pallavi Khatri, 'Forensic of an Unrooted Mobile Device', International Journal of Electronic Security and Digital Forensics, 12.1 (2020), 118-137 https://doi.org/10.1504/ijesdf.2020.10025327
2. Audibert M. L'extraction et l'exploitation des données contenues dans des supports numériques. Actualité juridique Pénal, 2023 p. 116.

3. Benoît A. La preuve numérique en procédure pénale: un système à (re)construire. Recueil Dalloz, 2023, p. 697.

4. Bruce Nikkel, 'NVM Express Drives and Digital Forensics', Digital Investigation, 16 (2016), 38–45 https://doi.org/10.1016/j.diin.2016.01.001

5. Cass. Crim., 12 juill. 2022, nos 21-83.710, 21-83.820, 21-84.096 et 20-86.652.

6. Cass. Crim., 30 avril 2024, n° 23-80.962

7. Digital Forensic Investigations in the Norwegian Police', Forensic Science International: Digital

8. Dubber-ley, S., Koenig, A., Murray, D. (eds.), Digital Witness – Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, Oxford University Press, Oxford, 2019, pp. 48-67.

9. Freeman, L., Vazquez Llorente, R., Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age, Journal of International Criminal Justice, Vol. 19, No. 1, 2021, pp. 163–188.

10. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings. Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c

11. Investigation, 40 (2022), 1-13 https://doi.org/10.1016/j.fsidi.2022.301351

12. Marchesi D., Intercepted Communications in the Ongwen Case: Lessons to Learn on Documentary Evidence at the ICC, International Criminal Law Review, Vol. 22, No. 5-6, 2022, pp. 920-940.

13. Michael Kohn, Mariki M. Eloff, and Jan Eloff, 'Integrated digital forensic process model', Computers and Security, 38 (2013), 103–115 https://doi.org/10.1016/j.cose.2013.05.001

14. Prosecutor v Al Mahdi, Case No. ICC-01/12-01/15-171

15. Prosecutor v Blagojević and Jokić, Case No. IT-02-60-T

16. Prosecutor v Dominic Ongwen, Case No. ICC-02/04-01/15, Judgment, 4 February 2021, para. 614 ff.

17. Prosecutor v Radislav Krstic, Case No. IT-98-33, Judgement, 2 August 2001, respectively paras. 237 and 253.

18. Prysiazhniuk I., Use of digital evidence in criminal process: some issues of right to privacy protection, Visegrad Journal on Human Rights, 5 (2023), 81-88 https://doi.org/10.61345/1339 7915.2023.5.11

19. Radina Stoykova, Stig Andersen, Katrin Franke, Stefan Axelsson, Reliability assessment of digital forensic investigations in the Norwegian police, Forensic Science International: Digital Investigation, Volume 40, 2022, 301-351

20. Reedy P., 'Digital Evidence Review 2016–2019', Forensic Science International: Synergy, 2 (2020) 489–520 https://doi.org/10.1016/j.fsisyn.2020.01.015

21. Report of the International Commission of Inquiry on Darfur to the United Nations Secretary-General, 2005, paras. 183 and 301 URL: https://www.legal-tools.org/doc/1480de/pdf/

22. Urvoas Jean-Jacques. Libres réflexions sur l'écriture de la loi. Actualité juridique Pénal, 2023, p. 85.

23. Vergès É. La preuve numérique, entre continuité et changement de paradigme. Revue Justice Actualités, ENM, n° 1, 2019.

24. Фігурський В.М. Докази в електронній формі у кримінальному провадженні. Галицькі студії. Юридичні науки. № 4, 2023. С. 97–105.

25. Мілімко Л.В., Жидовцев Я.В. Електронні докази в кримінальному судочинстві України. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. Випуск 88: частина 3 С. 302-308.

**Information about the author:**
**Marchenko Andriy Romanovych,**
Assistant Professor of the Department of Procedural Law
Yuriy Fedkovych Chernivtsi National University
2, Kotsiubynskoho St, Chernivtsi, 58012, Ukraine