ПРОБЛЕМА ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ/ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: НАУКОМЕТРИЧНИЙ ЗРІЗ

Кріцак Іван,
кандидат юридичних наук, доцент, старший науковий співробітник науково-дослідної лабораторії з проблем досудового розслідування, доцент кафедри кримінального права і кримінології Харківського національного університету внутрішніх справ

Рось Анна,
кандидат юридичних наук, доцент, старший оперуповноважений 1-го відділу управління боротьби з наркозлочинністю Головного управління Національної поліції у м. Києві

У травні 2023 року Європейський інститут права (ELI) опублікував проєкт Директиви про врегулювання взаємної прийнятності доказів, в тому числі електронних доказів, у кримінальному провадженні в Європейському Союзі, головною метою якого є сприяння розвитку європейського права в цій сфері. Серед основних положень: 1) докази, отримані в одній державі-члені, повинні бути прийнятими в іншій державі-члені без додаткових процедур або вимог, що підвищує ефективність та швидкість судових процесів; 2) окрема увага приділяється електронним доказам, враховуючи їх дедалі більшу роль у сучасних кримінальних розслідуваннях, з визначенням чітких правил щодо їх збору, зберігання та передачі між державами-членами; 3) наголошується на необхідності дотримання прав людини та основоположних свобод при зборі та використанні доказів, що включає захист персональних даних і забезпечення справедливого судочинства; 4) запровадження механізмів моніторингу та звітності для забезпечення прозорості процесу обміну доказами між державами-членами: створення централізованого реєстру для відстеження переміщення та використання доказів; запровадження програм підготовки та навчання для суддів, прокурорів та правоохоронних органів, спрямованих на підвищення обізнаності та розуміння нових правил та процедур [1].

Суд ЄС визнає, що доступ, зберігання та передача електронних персональних даних в досудовому провадженні, яке стає дедалі більш поширеним у кримінальному судочинстві, є втручанням у фундаментальні права на приватне та сімейне життя, і тому, якщо державний орган намагається отримати такі дані, це вимагає судового дозволу, який у всіх випадках повинен поважати принцип

пропорційності та встановлює, як критерій оцінки пропорційності, тяжкість злочинів [2].

Аналізуючи наукові праці іноземних авторів з означеного питання, не можна не погодитися з польським автором П. Левулісом, який наголошує, що цифрові докази стають дедалі популярнішими у кримінальних провадженнях – не лише щодо тих, які зазвичай називають «кіберзлочинами». Критерії правдивості таких доказів теоретично регулюються набором основних принципів, розроблених у рамках криміналістичної науки. Згідно з поточними теоретичними визначеннями, «цифрові докази» включають будь-яку інформацію доказової цінності, що зберігається або передається у формі цифрових даних. Очікується, що всі цифрові докази мають бути отримані та досліджені у судово-обґрунтований спосіб. Однак емпіричне дослідження, засноване на аналізі матеріалів польських кримінальних справ, засвідчує, що на практиці часто ігноруються певні вказівки цифрової криміналістичної експертизи щодо цифрових доказів, а інформація цифрового походження подається лише як роздруківки. Пропонується переоцінка поточного теоретичного визначення «цифрових доказів» на основі розрізнення між цифровими доказами в «загальному» (sensu largo) і «технічному» (sensu stricto) сенсі [3]. Цифрові докази повинні відповідати основним принципам криміналістичної науки, забезпечуючи їх достовірність та допустимість. З цих позицій важливим є те, що: – інформація має бути захищена від змін з моменту її вилучення до моменту представлення в суді; – підтвердження автентичності даних; – можливість незалежного відтворення процесу вилучення доказів іншими фахівцями; – детальний запис усіх дій, проведених із цифровими доказами.

У науковій праці «Електронний документ як джерело в кримінальному провадженні» авторами зазначається, що законодавець не завжди встигає за розвитком інформаційного суспільства, що призводить до неповного або недостатньо чіткого регулювання правовідносин, пов'язаних з використанням електронних документів, як доказів у кримінальних справах. Тож, важливо сформувати чітке та однозначне визначення електронного документа в законодавстві, яке б використовувалося в судовій та слідчій практиці, також необхідним вбачається створення методик і стандартів для збирання, збереження та використання електронних документів у кримінальних провадженнях [4].

У Китаї лише після внесення змін до кримінально-процесуального закону у 2012 році електронні дані були класифіковані як самостійний вид доказів, які можуть бути використані для підтвердження фактів злочину та включають: цифрові записи, електронні листи,

повідомлення в соціальних мережах, відео та аудіо файли, що можуть містити інформацію про подію злочину.

Попри те, що китайська влада доклала великих зусиль для інтеграції нових технологій в електронні дані та сформувала основу для регулювання електронних даних, у чинних нормах існують окремі недоліки: вразливі права підозрюваних у злочинах, відсутність департаменту спеціальних розслідувань, нечіткі положення у відповідних нормативних актах та неналежні механізми правового захисту [5].

У той час, як є важливим, щоб використання електронних доказів не порушувало права та свободи людини, що стосується як захисту конфіденційності, так і запобігання незаконному втручанню у приватне життя. Не менш важливою є також оцінка автентичності та цілісності електронних доказів. Це включає перевірку їхнього походження та відповідності встановленим стандартам, що мають передбачати процедури збору, зберігання, аналізу та представлення електронних доказів у суді [6].

Цифрова ера надає злочинцям безпрецедентні можливості для вчинення серйозних злочинів, починаючи від шахрайства та відмивання грошей і закінчуючи тероризмом. Злочини не лише вчиняються через кордони, навпаки, електронні докази можуть знаходитися за межами країни, яка їх шукає. Впродовж багатьох років правоохоронні органи та органи національної безпеки поставали перед труднощами в доступі до транскордонних електронних доказів, внаслідок чого країни шукали різні підходи до транскордонного доступу до доказів. Основна увага дискусії стосується різних підходів до правової бази, що регулює такий доступ. На підставі двох основних моделей управління, а саме моделі, яка виступає за вільний, відкритий, безпечний і глобальний Інтернет на основі захисту індивідуальних даних, і моделі кіберсуверенітету або багатосторонньої моделі, що дозволяє державі формулювати правила, засновані на ідеї суверенітету держави, що представляє своїх громадян, здійснено порівняльний аналіз і визначені їх переваги та недоліки. Так, у **США** – CLOUD Act дозволяє правоохоронним органам запитувати дані у компаній, незалежно від місця знаходження серверів. Серед переваг: швидкий доступ до даних для розслідування, недоліки – можливе порушення прав на приватність; в **ЄС** – GDPR і E-Evidence Regulation, переваги – високий рівень захисту персональних даних і міжнародна співпраця, недоліки – складність і тривалість процесу отримання даних; у **Китаї** передбачено суворий контроль за Інтернетом і даними всередині країни, з переваг – державний контроль і захист національних інтересів, недоліки – обмеження свободи Інтернету, можливі

порушення прав людини [7]. Цілком очевидно, що надмірна свобода в Інтернеті може ускладнювати боротьбу зі злочинністю. Водночас обмеження прав і свобод людини може переслідувати в тому числі різного роду політичні цілі.

Науковцями аналізуються найважливіші аспекти нового інструменту транскордонного співробітництва в рамках Європейського Союзу та у сфері кримінальних доказів, запропонованого Європейською Комісією. Адже стає дедалі більш поширеним, що органи держави-члена, що розслідують або переслідують конкретні кримінальні злочини, потребують отримання електронної інформації, що зберігається постачальником послуг, який заснований, представлений або пропонує свої послуги на території іншої держави-члена, незалежно від конкретного місця розташування даних. Основною визначальною особливістю моделі, прийнятої в пропозиції Комісії, є те, що сертифікат із розпорядженням про збереження або виготовлення електронних доказів буде надіслано безпосередньо законному представнику, призначеному постачальником послуг, який повинен буде надати швидку відповідь на орган, який дав відповідний запит. Втручання влади держави-виконавця передбачається лише в допоміжному та дуже винятковому порядку [8]. Загалом, регламент спрямований на те, щоб зробити процес отримання електронних доказів швидким та ефективним.

Висновки:

– використання електронних документів у кримінальному провадженні є важливим аспектом сучасної кримінальної юстиції. Потребує продовження робота над вдосконаленням правового регулювання та практичних аспектів їх застосування, що сприятиме підвищенню ефективності розслідування та судового розгляду кримінальних проваджень;

– виходячи з польського досвіду використання електронних доказів можна запропонувати відповідне нормативне розмежування цифрових доказів в загальному сенсі – будь-яка цифрова інформація, що використовується в ході досудового розслідування або судового розгляду, та в технічному сенсі – дані, які були отримані, збережені та проаналізовані відповідно до всіх криміналістичних стандартів, що забезпечують їхню цілісність, достовірність та допустимість у суді;

– враховуючи досвід застосування електронних даних у Китаї, слід зосередитися на подальшому захисті прав учасників кримінального процесу та забезпеченні гармонійної взаємодії між новими технологіями й теорією доказів, що може включати створення спеціалізованих відомств, уточнення нормативних актів і розробку нових механізмів правового захисту;

– ефективне управління глобальним кіберпростором потребує балансу між безпекою та правами людини. Розробка правової бази для транскордонного доступу до електронних доказів повинна враховувати як національні інтереси, так і міжнародні стандарти захисту прав людини.

Література:

1. Santos AM. Mutual admissibility of cross-border criminal evidence in the european union: the european law institute draft directive proposal. *Revista general de derecho procesal.* 2023.
2. Vall-Ilovera, SOI. Access to personal data held by electronic communications service providers in criminal investigations according to the Court of Justice of the *Eu. idp-internet law and politics.* 2020.
3. 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. № 13 (4). PP. 403–417.
4. Manzhai O, Lysenko A, Chycha R. Electronic Document As A Source In Criminal Proceedings. *International journal of computer science and network security*. 2022. № 22 (3). PP. 629–633.
5. Yang F, Feng J. Rules of electronic data in criminal cases in China. *International journal of law crime and justice*. 2021.
6. Du J, Ding LP, Chen GX. Research on the Rules of Electronic Evidence in Chinese Criminal Proceedings. *International journal of digital crime and forensics*. 2020. № 12 (3). PP. 111–121.
7. Watney M. Analysing Different Approaches to Cross-Border Electronic Evidence Data-Sharing in Criminal Matters. 14th International Conference on Cyber Warfare and Security (ICCWS). *Proceedings of the 14th international conference on cyber warfare and security*. 2019. PP. 484–491.
8. Sancho MD. Reflections on the proposal for eu regulation on european production and preservation orders for electronic evidence in criminal matters. *Revista general de derecho procesal.* 2022.