МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА

Правові горизонти

Legal horizons

ВИПУСК 15 (28)

Суми – 2019

DOI: http://www.doi.org/10.21272/legalhorizons.2019.i15.p86

ОСОБЛИВОСТІ ДОСТУПУ ДО СОЦІАЛЬНИХ МЕРЕЖ ТА ЇХНЬОГО ВИКОРИСТАННЯ ЯК ЕЛЕМЕНТ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Мезенцева Анастасія Андріївна,
Факультет правничих наук,
Національний університету «Києво-Могилянська академія»

Стаття присвячена дослідженню теоретичних та практичних проблем механізму правового регулювання доказової бази у кримінальному процесуальному праві. У статті досліджені проблеми визнання відкритої інформації, поширеної у соціальних мережах, як доказової бази. Акцентується увага на вичерпному переліку процесуальних джерел доказів у кримінальному процесуальному праві.

Інформаційні технології розглянуті як внесок у розвиток науки кримінального процесуального права. Ці технології та інші сучасні девайси мають відображення на будь-якому суспільстві з позитивної сторони, так і з негативної. Швидкий розвиток технологій зумовив пришвидшення роботи з документами, але водночас і збільшення кількості злочинів, вчинених із використанням електронно-обчислювальних машин. Суспільство стало грамотнішим у цифровому вимірі, але кіберзлочинці теж не стоять на місці.

Поки що ця тема не достатньо досліджена, що не сприяє остаточному вирішенню проблем, які виникають під час практичної діяльності. Однозначним є те, що кримінальне процесуальне право має перейняти та включити до переліку процесуальних джерел доказів електронні докази, передбачені у цивільному процесуальному праві та господарському процесуальному праві.

Єдиної спільної точки зору немає і у західних вчених. У статті наведена практика українських та іноземних судів для висвітлення проблемного питання, пов'язаного із необхідністю встановити та законодавчо закріпити місце інформації, отриманої з відкритих джерел.

Особлива увага приділяється слідчим діям, оскільки електронні докази потрібно виявляти, фіксувати та досліджувати визначеним законом шляхом, а також їх необхідно правильно зберігати.

На підставі дослідження численних точок зору науковців, зроблено висновок, що інформація з відкритих джерел могла би становити різновид слідчих дій, тому потрібно реформувати положення Кримінального процесуального кодексу України.

Ключові слова: злочинність, тенденції, діджиталізація, соціальна активність.

Mezentseva A. A. Features of access to social networks, and their use as the elements of secret investigative proceedings. The article is devoted to the research of theoretical and practical problems of the mechanism of evidence base regulation in the Criminal Procedural Law. The article deals with the problems of recognition of an open-source information that is spread in social networks as the base of proof.

Information technologies are considered as a contribution to the development of the science of criminal procedural law. These technologies and other modern devices are reflected in any society within their positive and the negative sides. The rapid development of technologies led to the faster work with documents. But at the same time, they increased the number of crimes committed with the use of

electronic devices. Society has become more literate in digital terms, however, cybercriminals are also not stative.

So far, this topic has not been sufficiently investigated, which does not contribute to the final resolution of the problems that arise during practical activities. It is reasonable that criminal procedural law should adopt and include in the list of procedural sources of evidence electronic evidence as provided in civil procedural law and commercial procedural law.

There is no single common point of view among Western scholars also. The article describes the practice of Ukrainian and foreign courts in order to cover a problematic issue related to the need to establish and legally secure the place of information obtained from open sources.

Special attention is paid to investigative actions, since electronic evidence needs to be detected, recorded and explored by law, and has to be properly stored.

Based on the research of many scientists' viewpoints, it was concluded that information from open sources could be a kind of investigative actions, therefore, it is necessary to reform the provisions of the Criminal Procedure Code of Ukraine.

Keywords: criminality, tendencies, digitalization, social activity.

Постановка проблеми. Розвиток інформаційних технологій зумовлює необхідність відповідного розвитку кримінального процесуального законодавства. Нині дослідження цієї сфери не відповідають дійсності враховуючи, що оцифровування діяльності індивіда та суспільства відбувається значно швидше, ніж українська кримінально-процесуальна наука має змогу реагувати.

Виклад основного матеріалу. Глобалізація зумовила надшвидкий розвиток суспільства. Особливо це відображено у розширенні використання електронно-обчислювальних машин та різних девайсів. Тому, одним із головних трендів сучасності є діджиталізація.

Діджиталізація має безліч варіацій у різних сферах життєдіяльності, особливо у бізнесі. Однак, за загальним правилом, це - явище, яке походить від слова «цифровий» (англ. «digital»). Діджиталізація – це «використання цифрових – інформаційно-комунікаційних технологій» [11, с. 119].

Суспільство все частіше використовує новітні можливості, і це знайшло відображення не тільки у повсякденному житті. Оскільки сектор інформаційних технологій в Україні та усьому світі «став потужною галуззю національної економіки», яка має велику динаміку розвитку, що «ініціює потужний технологічний імпульс у решту галузей» [11, с. 123].

Окремі аспекти правового регулювання кіберзлочинів та електронних доказів становили предмет наукових пошуків вчених: Азаров Д.С., Білоус В.В., Дудоров О.О., Калиновський О.В., Коваленко В.В., Крапивін Є.О., Купка Ю.М., Музика А.А., Пивоваров В.В., Письменний Д.П., Тарасенко Н.Ю., Удалова Л.Д., Школьніков В.І. та інші.

У кіберзлочинах електронні системи та девайси можуть застосовуватись по-різному: як об'єкт злочину, як інструмент вчинення злочину або як сховище для джерел процесуальних доказів, які мають відношення до вчиненого злочину [7, с. 1].

Ці технології значно полегшили також можливість вчинення злочинів. Набули поширення види шахрайства із використанням електронно-обчислювальних машин. Відповідно до статистичних даних, наведених Генеральною прокуратурою України на запит на доступ до публічної інформації, упродовж 2016 року було зареєстровано 705 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, передбачених статтями 361-363-1 Кримінального кодексу України [12]. Упродовж 2017 року кількість зросла до 3178 злочинів [13].

Отож, яким чином би змінилась ситуація, якщо застосовувати інформацію, викладену у соціальну мережу у відкритий доступ, можна було використовувати в якості допустимого доказу?

У частині 1 статті 214 Кримінального процесуального кодексу України (далі – КПК України) зазначено, що слідчий, прокурор невідкладно, але не пізніше 24 годин 1) після подання заяви, повідомлення про вчинене кримінальне правопорушення або 2) після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, зобов'язаний внести відповідні відомості до Єдиного реєстру досудових розслідувань, розпочати розслідування та через 24 години з моменту внесення таких відомостей надати заявнику витяг з Єдиного реєстру досудових розслідувань [1].

Тобто, або за допомогою сторонньої особи, або прокурор, слідчий самостійно виявляє з будь-якого джерела. «Будь-яке джерело» - це, насправді, вичерпний перелік процесуальних джерел доказів. Цей перелік процесуальних джерел доказів зазначено у частині 2 статті 84 КПК України, а саме: показання, речові докази, документи, висновки експертів [1]. Жодних інших доказів КПК України не передбачає.

Проте, інші поняття доказів висвітлені у інших нормативно-правових актах України. Наприклад, параграфом 5 розділу 5 Цивільного процесуального кодексу України висвітлена нова категорія доказів - електронні докази. У частині 1 статті 110 ЦПК України визначено, що електронні докази – це «інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет)» [4]. Таким чином, ЦПК України не виключає можливість використання веб-сторінок соціальних мереж як доказів. Подібним чином, положення статті 96 Господарського процесуального кодексу України містить, навіть дублює, наведене вище поняття [5].

У одній цивільній справі 2015 року Голосіївський районний суд міста Києва визнав факт порушення майнових прав інтелектуальної власності, зафіксований позивачем за допомогою онлайн-сервісів збереження змісту веб-сторінок [14]: «Знімки веб-сторінки, зроблені за допомогою онлайн-сервісів збереження змісту веб-сторінок, здійснюються за допомогою програмного забезпечення, розміщеного на сервері відповідної незаангажованої особи. Відповідний файл зі знімком також зберігається на сервері такої особи та розміщується в публічному доступі у мережі Інтернет. Разом зі знімком фіксується оригінальна адреса веб-сторінки та точний час, коли його було зроблено. При цьому копіюється безпосередньо та інформація, яка знаходиться на веб-сторінці, а не її відображення на екрані користувача. У такий спосіб фактично виключається можливість модифікації оригінального змісту веб-сторінки, адже всі операції, пов'язані з фіксацією змісту веб-сторінки і її збереженням, здійснюються без втручання будь-яких зацікавлених осіб».

У зв'язку з цим, необхідно детальніше розглянути можливість використання інформації, що знаходиться у відкритому доступі. Що стосується кримінального провадження, то інформація з відкритих джерел також надала б можливість пришвидшити розслідування злочинів. Розглядуваний вид інформації міг би у майбутньому становити різновид слідчих (розшукових) дій.

Слідчі дії, як один із основних способів збирання доказів, знаходиться поруч із процесом доказування у кримінальному провадженні, адже йому передує одне завдання – «отримання (збирання) доказів або перевірка вже отриманих доказів» [3, с. 223]. Тому, розмежуємо наступні поняття: слідчі дії, слідчі (розшукові) дії та негласні слідчі (розшукові) дії.

Слідчі дії – це дії, які регламентовані нормами процесуального права, здійснюються уповноваженою особою в межах кримінального процесуального провадження з дотриманням законних вимог, супроводжуються необхідним документуванням, і є «комплексом пізнавально-засвідчувальних операцій, спрямованих на отримання, дослідження й перевірку доказів» [2, с. 325].

Слідчі (розшукові) дії, відповідно до частини 1 статті 223 КПК України, є «діями, спрямованими на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні» [1]. Їх основу становлять – візуальне спостереження, розпитування, сприйняття, пошук, порівняння (ідентифікація), відтворення, дослідження, тобто, окремі методи пізнання, які «супроводжуються закріпленням (фіксацією та засвідченням) одержаної доказової інформації чи висновків у відповідних процесуальних документах» [2, с. 325].

Негласні слідчі (розшукові) дії – це «різновид слідчих (розшукових) дій, відомості про факт і методи проведення яких не підлягають розголошенню, спрямовані на збирання, перевірку чи дослідження фактичних даних у конкретному кримінальному провадженні, та які проводяться у разі крайньої необхідності, коли відомості про злочин та особу, яка його вчинила, неможливо отримати іншим шляхом» [2, с. 421].

Іншими словами, виникає питання стосовно пропорційності отримання інформації такого виду та релевантності здобутих фактичних даних. Робота з такою інформацією має сприйматись як аналітична.

Водночас, міжнародний досвід у цьому аспекті також не є однозначним, хоча свідчить про те, що все це є можливим.

Одним із прикладів можна навести, коли Нью-Брансвікський суд Канади визнав у кримінальній справі R. v. Soh (G.N.) допустимим доказом скріншот із мережі Facebook [6, с. 754]. Суд у цій кримінальний справі визнав, що «дефініція «електронний документ» охоплює всі документи в електронному форматі, які містяться в електронній пошті, всі комп'ютерні файли, метадані цих файлів, історію браузера, інформацію, яка розміщена онлайн на веб-форумах таких сайтів, як Twitter та Facebook, текстові повідомлення, онлайн-листування тощо» [6, с. 754].

Іншим прикладом можна навести випадок, коли окружний суд штату Пенсільванії визнав, що «докази, отримані в соціальних мережах, треба розглядати як будь-які інші фотографії», у відповідності до законодавства США [6, с. 755].

Нині, навіть емодзі займають значне місце у людському житті, а саме – у спілкуванні у соціальних мережах. Професор юриспруденції Університету Санта-Клари Ерік Голдман дослідив використання емодзі під час судового розгляду у США у період з 2004 по 2019 роки і з'ясував, що їх використання зростає: «на 2018 рік припало 30% випадків» [10]. Американська веб-сторінка про технології та культуру The Verge відзначила, що «у результаті інтерпретація емодзі відіграла не ключову роль у розслідуванні, але зміцнила доказову базу обвинувачення» [10].

Стаття 264 КПК України передбачає зняття інформації з електронних інформаційних систем у якості одного із видів негласних слідчих (розшукових) дій [1]. Це є відносно новою слідчою дією для українських правоохоронних органів. Поява такої слідчої дії була зумовлена розвитком нових інформаційних технологій, а її зміст полягає у «одержанні (зокрема із застосуванням технічного обладнання) інформації, що міститься в електронно-обчислювальних машинах, зберігалась на персональному комп'ютері або кількох персональних комп'ютерах, об'єднаних у локальну мережу, або ж на зовнішніх накопичувачах інформації, що приєднувались до електронних інформаційних систем, в автоматичних системах або комп'ютерних мережах» [2, с. 441].

Зауважимо, що існують фактичні та юридичні підстави для зняття цієї інформації, і їх необхідно розмежувати.

Фактичними підставами є «фактичні дані, що вказують на наявність в електронній інформаційній системі або її частині даних, які мають значення для кримінального провадження» [2, с. 441].

Однією з юридичних підстав зняття інформації з електронних інформаційних систем є дозвіл власника, володільця або утримувача такої електронної системи [2, с. 442].

У результаті цього виникає наступне питання: наскільки це співвідноситься із правом особи не свідчити проти себе?

Відповідно до пункту 12 Постанови Пленуму Верховного Суду України «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» від 27.02.2009 р. № 1, належним відповідачем у разі поширення оспорюваної інформації в мережі Інтернет є автор відповідного інформаційного матеріалу та власник веб-сайта [14].

В оглядовому листі Вищого господарського суду України № 01-06/770/2014 від 12.06.2014 року «Про деякі питання практики застосування господарськими судами законодавства про інформацію» передбачено, що «за поширення в Інтернеті анонімної та недостовірної інформації відповідає власник веб-сайту, на якому розміщено матеріал, оскільки саме він створив технологічну можливість та умови для поширення такої інформації» [14].

Водночас, інформація, поширена у мережі Інтернет, знаходиться у відкритому доступі, - є загальнодоступною. Особа добровільно розміщує інформацію про себе на своїй сторінці у соціальній мережі. Відповідно до цього, «для зняття інформації, розміщеної на загальнодоступних соціальних сайтах Інтернету, дозволу слідчого судді чи прокурора не потрібно, оскільки в цьому разі не відбувається втручання у приватне спілкування чи приватне життя» [2, с. 442].

Окрім цього, дана інформація може використовуватись для збору інформації про саму особу, наприклад, для встановлення мотиву злочину. Використання соціальних мереж для виявлення мотиву злочину є «порівняно новим джерелом інформації» [9, с. 211]. За доступними на соціальній сторінці відомостями, на нашу думку, «можна дати початкову психологічну та моральну характеристику її користувача (за умови, що він особисто її наповнює)» [9, с. 211].

До того ж, розглядувану інформацію можна використовувати як цифрове алібі [8, с. 145]. Існує таке поняття як «інтероперабельність», тобто «можливість оперувати з будь-якого місця», підключеного до мережі Інтернет [11, с. 125]. У зв'язку з цим, теоретично, можна відстежити особу у певний період часу, не втручаючись до її приватного життя, а лише користуючись інформацією з її соціальних мереж.

Висновки. З метою покращення становища правоохоронних органів та їхньої взаємодії із стороною захисту, з метою пришвидшення проведення необхідних для відповідних видів слідчих дій, пропоную доповнити положення статті

61 КПК щодо процесуальних джерел доказів та розділи КПК, присвячені проведенню слідчих дій, електронними доказами, а саме – інформацією з відкритих джерел.

Література :

1. Кримінальний процесуальний кодекс України №4651-VI, Редакція від 10.11.2018, підстава 2599-VIII. [Текст] / Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88. // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17

2. Науково-практичний коментар Кримінального процесуального кодексу України. Вид. 14-те, доповн. і перероб. – К.: Правова Єдність, 2017. – 828 с.

3. Кримінальний процес: підр. [Текст] За заг. ред. В.В. Коваленка, Л.Д. Удалової, Д.П. Письменного. – К. – "Центр учбової літератури", 2013. – 544 с.

4. Цивільний процесуальний кодекс України №1618-IV, Редакція від 04.11.2018, підстава 2581-VIII. [Текст] / Відомості Верховної Ради України (ВВР), 2004, № 40-41, 42, ст.492. // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/1618-15

5. Господарський процесуальний кодекс України №1798-XII, Редакція від 28.08.2018, підстава - 2475-VIII. [Текст] / Відомості Верховної Ради України (ВВР), 1992, № 6, ст.56. // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/1798-12

6. Калиновський О.В., Школьніков В.І. Процесуальний порядок здобуття відомостей з електронних інформаційних систем, доступ до яких не обмежується, та їх статус у кримінальному судочинстві. [Текст] / Кримінальний процесуальний кодекс 2012 року: ідеологія та практика правозастосування: колективна монографія. / Проблеми забезпечення ефективності досудового розслідування. / За заг. ред. Ю.П. Аленіна; відпов. за вип. І.В. Гловюк. – Одеса: Видавничий дім «Гельветика», 2018. – 1148 с. – с. 753-773. // [Електронний ресурс]. – Режим доступу:
http://dspace.onua.edu.ua/bitstream/handle/11300/9497/Kol_monogr_CPC2012.pdf?sequence=1#page=753

7. Venansius Baryamureeba, Florence Tushabe. The Enhanced Digital Investigation Process Model. [Текст] / The Digital Forensic Research Conference: DFRWS, 2004, USA, Baltimore, MD. – с. 1-9. // [Електронний ресурс]. – Режим доступу: https://dfrws.org/sites/default/files/session-files/paper-the_enhanced_digital_investigation_process_model.pdf

8. Тарасенко Н.Ю., Купка Ю.М. Окремі засоби збирання криміналістичної інформації. [Текст] / Правові горизонти. – Суми. – 2016. - с. 142-147. // [Електронний ресурс]. – Режим доступу: http://essuir.sumdu.edu.ua/handle/123456789/57859

9. Цюприк І.В. Особивості встановлення винуватості осіб, причетних до вчинення терористичних актів. [Текст] // [Електронний ресурс]. - Режим доступу: https://ojs.naiau.kiev.ua/index.php/scientbul/article/view/777/782

10. Чи можна емодзі приймати як докази? [Текст] // [Електронний ресурс]. Режим доступу: https://telegra.ph/CHi-mozhna-emodzi-prijmati-yak-dokazi-03-02

11. Дульська І. В. Цифрові технології як каталізатор економічного зростання. [Текст] / І. В. Дульська // Економіка і прогнозування. - 2015. - № 2. - с. 119-133. // [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/econprog_2015_2_11

12. Статистика кіберзлочинів зареєстрованих правоохоронними органами в Україні в 2016 році та у січні - квітні 2017 року. [Текст] // [Електронний ресурс]. Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v

13. Статистика кіберзлочинів зареєстрованих правоохоронними органами в Україні в 2017 році. [Текст] // [Електронний ресурс]. Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v_2

14. Справа № 752/9476/15-ц, провадження № 2/752/4249/15. [Текст] // [Електронний ресурс]. Режим доступу: http://reyestr.court.gov.ua/Review/52726541