РОЗДІЛ 9
КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.98

ДО ПИТАННЯ ДОКАЗОВОЇ СИЛИ КІБЕРІНФОРМАЦІЇ В АСПЕКТІ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

THE QUESTION PROBATIVE CYBERINFORMATION IN ASPECTS OF INTERNATIONAL COOPERATION IN CRIMINAL PROCEEDINGS

Ахтирська Н.М.,
кандидат юридичних наук, доцент кафедри правосуддя юридичного факультету Київського національного університету імені Тараса Шевченка

Стаття присвячена висвітленню проблем, пов'язаних із визначенням доказової сили кіберінформації, одержання якої відбувається під час міжнародного співробітництва у кримінальному провадженні. Автор звертає увагу на принцип співвідношення анонімності в Інтернеті з іншими правами та інтересами.
Ключові слова: міжнародне співробітництво під час кримінального провадження, кіберінформація, Інтернет, докази.

Статья посвящена проблемам определения доказательственной силы киберинформации, полученной в рамках международного сотрудничества по уголовным делам. Автор акцентирует внимание на принципе соотношения анонимности в Интернете с другими правами и интересами.
Ключевые слова: международное сотрудничество по уголовным делам, киберинформация, Интернет, доказательства.

The article is devoted to problems of determining probative value of cyberinformation obtained in framework of international cooperation in criminal matters. The author focuses on principle of correlation of anonymity on Internet with other rights and interests.
Key words: international cooperation in criminal matters, value of cyberinformation, Internet proof.

Актуальність теми. Американський винахідник і бізнесмен Чарльз Кеттерінг переконливо закликав думати про майбутнє, оскільки нам доведеться провести там решту свого життя [1, с. 2]. Варто визнати, що ми живемо в цифрову еру, яка все більше видозмінює усталені способи створення інформації, її передачі, знищення, а також використання. Це зумовлює потребу пристосовувати правову систему до кіберпростору. Прийняття Кримінального процесуального кодексу України суттєво змінило процедуру збору доказів, однак невирішеним залишилось питання використання електронних доказів.

Йдеться, зокрема, про визначення електронних доказів, способи їх одержання, визначення їх належності, допустимості, можливості використання міжнародної правової допомоги в розкритті IP-адрес користувачів світової мережі у випадку підозри щодо вчинення ними кримінальних правопорушень тощо. Вказані питання досліджували М.В. Салтевський [2], О.Г. Волеводз [3], Б.В. Анрєєв, П.Н. Пак, В.П. Хорст [4], В.О. Голубєв, Т.А. Сайтарли [5] та інші. Разом із тим слід визнати, що у вітчизняній науці кримінального процесу та криміналістики недостатньо приділено уваги розробці концепції кібердоказів, незважаючи на те, що слідча та судова практика вкрай потребує не тільки правового визначення, тлумачення, але й науково-методичного забезпечення кримінального провадження в даній категорії злочинів, а особливо у сфері міжнародного співробітництва. Саме тому метою статті є теоретична розробка концепції електронних доказів, з'ясування напрямів імплементації конвенційних вимог у законодавство України щодо боротьби з кіберзлочинністю.

Виклад основного матеріалу. Виникнення цифрового простору, де щохвилини створюється додаткова інформація, авторами та користувачами якої є незліченна кількість осіб з усього світу, створило так званий кіберландшафт, який абсолютно не можна оцінювати усталеними поняттями, що застосовуються в реальному світі. Виникла проблема балансу прав людини, конфіденційності, анонімності та безпеки держави і суспільства. Наукова дискусія з цього приводу набула гостроти після того, як Джуліан Ассандж оприлюднив секретну інформацію про військові злочини, шпіонські скандали, корупцію високопосадовців, за що його оголошували в міжнародний розшук, звинувачували, заарештовували, судили. Едвард Сноуден, американський технічний спеціаліст, колишній співробітник ЦРУ та Агентства національної безпеки США розкрив секретну інформацію, яка стосується тотального слідкування американських спецслужб за інформаційними кому-

нікаціями громадян багатьох держав за допомогою інформаційних мереж та мереж зв'язку, у тому числі дані про проекти PRISM, X-Keyscore и Tempora. За даними доповіді Пентагону, Сноуден викрав 1,7 млн. секретних файлів, які стосуються життєво важливих операцій американської армії, флоту, морської піхоти та військово-повітряних сил [6]. Сноудену заочно пред'явлено обвинувачення в шпіонажі та викраденні державної власності, він оголошений у міжнародний розшук.

У зв'язку з цим постають питання, що таке докази в інформаційних технологіях, яким чином їх одержувати, оцінювати та використовувати.

Відповідно до ст. 84 КПК України доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому законом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню (ч. 1). Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів (ч. 2). У ст. 99 КПК України дається визначення, згідно з яким документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження (ч. 1). Зокрема, до документів можуть належати: 1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні); 2) матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надано Верховною Радою України (ч. 2). Наведене свідчить, що законодавець допускає використання електронних носіїв інформації, проте уточнює, що доказ має бути матеріальним об'єктом. Цифрові технології використовують віртуальний простір, а тому носієм (фіксатором) інформації може бути беззаперечно матеріальний об'єкт, однак при цьому варто уточнити, що навіть сама інформація у віртуальному просторі також має визнаватися доказовою. Як свідчить слідча практика, досить часто виникає можливість виявляти правоохоронним органам ознаки вчинення кримінального правопорушення певними особами, переглядаючи відкриті офіційні сайти інших держав. Наприклад, державний службовець, який за законодавством України не має права бути підприємцем, за кордоном зареєстрований як власник комерційної структури. Джерелом у даному випадку є офіційний реєстр органу виконавчої влади іноземної держави. В даному випадку правоохоронні органи ставлять слушне запитання, чи варто ускладнювати процедуру притягнення до відповідальності особи за вчинення корупційного правопорушення надсиланням запиту до іноземної держави про надання письмового варіанту документа (виписки з Реєстру підприємців), чи достатньо електронної інформації, яку можна одержувати з відкритих іноземних джерел.

На нашу думку, міжнародне співробітництво під час кримінального провадження на підставі запитів має здійснюватися лише у тому випадку, коли самостійне одержання інформації може завдати шкоди суверенітету держави, а тому здійснюється лише уповноваженими на те іноземними органами. А коли потрібна інформація міститься у відкритому віртуальному просторі, який не має визначених меж, то достатньою є лише електронна форма факту. Це стосується й випадків розміщення в Інтернеті на офіційних сайтах державних органів іноземних держав фотографій, на яких зображуються високопосадовці, які вручають або одержують цінні подарунки. Це є підставою для подальшої перевірки, куди скеровується цей предмет – до установи, яку під час офіційного візиту представляє посадовець (як встановлено законом), чи привласнює його (що має ознаки корупційного правопорушення).

Відповідно до ст. 264 КПК України пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування (ч. 1). При цьому не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем, або не пов'язаний з подоланням системи логічного захисту (ч. 2) [7]. Так, в одному з кримінальних проваджень слідчий за погодженням з прокурором звернувся до суду з клопотанням про застосування запобіжного заходу у вигляді тримання під вартою громадянина З., однак підозрюваний в судове засідання не з'явився з причин, які слідчим суддею були визнані як неповажні. Підставою для цього, зокрема, був рапорт оперуповноваженого про те, що переглядом сторінки в мережі інтернет «Facebook» встановлено, що З. знає про відкрите щодо нього кримінальне провадження і дату розгляду вказаного питання в суді, але підозрюваний коментує свої виклики до правоохоронних органів і викладає вручені йому повістки на своїй сторінці в мережі «Facebook». На підставі цього слідчий суддя прийняв рішення про здійснення приводу, оскільки неявка визнана неповажною.

У випадку необхідності одержання інформації з закритих джерел або розкриття IP-адрес користувачів потрібне рішення слідчого судді про доступ до таких даних. Так, до провадження слідчого судді надійшло клопотання прокурора про надання дозволу на отримання тимчасового доступу до речей та документів, які перебувають у адміністрації соціальної мережі: «www.facebook.com», розташованому за адресою: Facebook Inc. 10 Brock Street, NW1 3FG London, United Kindom 1601 Willow Road Menlo Park, CA 94025 United States. Обґрунтовуючи внесене клопотання, прокурор вказав, що прокуратурою про-

водиться досудове розслідування у кримінальному провадженні за ознаками кримінального правопорушення, передбаченого п. 12 ч. 2 ст. 115 КК України. Слідчий зазначив, що по даному кримінальному провадженні провадяться слідчі дії, в зв'язку з чим виникла необхідність в отриманні доступу до документів, які перебувають у адміністрації соціальної мережі: «www.facebook.com». Слідчий суддя, розглянувши дане клопотання у відсутність особи, у володінні якої знаходяться речі і документи, на підставі ч. 2 ст. 163 КПК України прийняв рішення про надання дозволу на доступ до документів. Окрім цього було ухвалено, що службовим особам адміністрації соціальної мережі «www.facebook.com» надати (забезпечити) тимчасовий доступ до речей і документів, особам, які здійснюють досудове розслідування у кримінальному провадженні та/або оперативним підрозділам органів внутрішніх справ, які здійснюють слідчі (розшукові) дії в кримінальному провадженні за письмовим дорученням слідчого, прокурора та надати їм можливість вилучити зазначені в ухвалі копії документів. У разі невиконання ухвали про тимчасовий доступ до речей і документів слідчий суддя, суд за клопотанням сторони кримінального провадження, якій надано право на доступ до речей і документів на підставі ухвали, має право постановити ухвалу про дозвіл на проведення обшуку з метою відшукання та вилучення зазначених речей і документів.

Однак, як свідчить слідча практика, адміністрація Yahoo (офіс в Каліфорнії) та ін. не надають таку інформацію, вважаючи, що такі вказівки на доступ до інформації є порушенням суверенітету, а ухвали іноземних судів безпідставними, оскільки імперативність рішень національних судів діє в межах державних кордонів. Така ситуація пояснюється тим, що Конвенція про кіберзлочинність, яка передбачає процедуру термінового збереження комп'ютерних даних, термінового розкриття збережених даних про рух інформації; взаємну допомогу щодо доступу до комп'ютерних даних; транскордонного доступу до даних, які зберігаються, коли вони є публічно доступними, взаємну допомогу у збиранні даних про рух інформації у реальному часі; взаємну допомогу у перехопленні даних змісту інформації [8], на жаль, ратифікована лише у 46 з-поміж 195 держав в усьому світі.

Електронні докази мають спільні риси з традиційними доказами, але водночас мають низку унікальних характеристик: 1) їх не видно неозброєним оком: вилучити їх, зачасти, може лише спеціаліст; 2) вони є нестійкими, за певних обставин інформація в пам'яті пристрою може бути змінена або втрачена. Наприклад, при розрядці пристрою або недостатності пам'яті система накладає (записує) нову інформацію замість попередньої, а це значить, що й докази можуть бути знищені. Комп'ютерна пам'ять може бути пошкоджена або знищена під впливом фізичних факторів (високий рівень вологості, висока температура) та електромагнітних хвиль; 3) вони можуть бути змінені або знищені в процесі експлуатації пристрою: пам'ять комп'ютера постійно змінюється на команду користувача («зберегти», «знищити») або операційної системи; 4) їх можна копіювати без втрати якості необмежену кількість разів, й будь-яка наступна копія не буде відрізнятися від оригіналу. Завдяки цій унікальній особливості різні спеціалісти можуть паралельно й одночасно досліджувати копії одного й того ж документа, не торкаючись оригіналу; 5) нові технології розвиваються з великою швидкістю, а тому методи й процедури збору та дослідження електронних доказів мають постійно оновлюватися.

Висновки. На законодавчому рівні необхідно закріпити, що електронні докази – це дані, які підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем, у тому числі програми виконання комп'ютерною системою або інших дій. Джерелами електронних доказів доцільно визнавати електронні пристрої: комп'ютери, периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери та інші портативні пристрої, в тому числі мережу Інтернет. Інформація з цих джерел не має фізичної форми. В рамках міжнародного співробітництва необхідно інтенсифікувати використання електронних способів передачі інформації, безпосередньо електронної віртуальної інформації.

Конвергенція правових концепцій, зміни в законодавстві інших держав суттєво впливають на національне правотворення в умовах глобалізації, позитивно діють на розвиток законодавства в Україні. Практика правоохоронних органів та суду дає можливість виявляти прогалини в нормах, які визначають процес збору доказів (зокрема, електронних), що слугуватиме стимулом до змін у кримінальному процесуальному законодавстві.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Шмідт Е., Коен Дж. Новий цифровий світ: як технології змінюють державу, бізнес і наше життя / Переклад з анг. Ганна Лелів. – Львів : Літопис, 2015. – 368 с.

2. Салтевский М.В. Осмотр компьютерных средств на месте происшествия: методические рекомендации/ М.В. Салтевский. – Х. : АПрНУ, 1999. – 11с.

3. Волеводз А.Г. Противодействие компьютерным преступлениям / А.Г. Волеводз. – М. : Юрлитинформ, 2002. – 496 с.

4. Андреев Б.В., Пак П.Н., Хорст В.П.. Расследование пре ступлений в сфере компьютерной информации / Б.В. Андреев, П.Н. Пак, В.П. Хорст. – М. – : Юрлитинформ, 2001. – 152 с.

5. Голубев В.А., Сайтарлы Т.А. Организационно-правовые аспекты противодействия компьютерной преступности и кибертерроризму // Информационные технологи и информационная безопасность в науке, технике и образовании. – Киев–Севастополь: НТО РЭС Украины, 2004. – 332с.

6. Пентагон подсчитал, что Э. Сноуден похитил 1,7 млн секретных файлов. [Електронний ресурс] – Режим доступу: http://www.rbc.ru/politics/10/01/2014/898589.shtml.

7. Кримінальний процесуальний кодекс України від 13.04.2012 р. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/4651-17.

8. Конвенція про кіберзлочинність Ради Європи від 23.11.2001 р. Ратифікація від 07.09.2005. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575.