

УДК 343.141.2

Юлія Олегівна ШИШАЦЬКА,

студентка 1 курсу магістратури

факультету прокуратури та слідства (кримінальної юстиції)

Національного університету «Одеська юридична академія»

РЕГЛАМЕНТАЦІЯ ЕЛЕКТРОННИХ ДОКАЗІВ В СУЧАСНОМУ ЗАКОНОДАВСТВІ ЯК ЗАСІБ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Сьогодні стрімкий розвиток новітніх цифрових технологій в ІТ-сфері значно відображається у повсякденному житті та відкладає свій відбиток на правові інститути. Зростаючий рівень зацікавленості та використання мережі Інтернет через електронні прилади підвищує ризик загрози прогресування кіберзлочинності. Саме в той час з'являються нові типи злочинів, нові способи та засоби їх вчинення, склад злочину перетворюється частиною нового віртуального простору. Доказування таких злочинів починає викликати багато питань та труднощів через недосконалість діючого кримінального законодавства та недостатню урегульованість інституту електронних доказів. Відповідно, враховуючи новизну нормативної регламентації електронних доказів у чинному українському законодавстві, слід проаналізувати їх регламентацію в кримінальному, цивільному та адміністративному судочинстві, зокрема, розмежування їх на види.

У ст. 100 Цивільного процесуального кодексу України електронні докази поділяються на: електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи і т.д.); веб-сайти (сторінки); текстові, графічні, голосові повідомлення; метадані; бази даних; інші дані в електронній формі [1].

Саме така форма поділу не є коректною, тому що зміст цих електронних доказів зникає як такий, натомість з'являється узагальнююче поняття – «електронний документ», що регулюється Законом України «Про електронні документи та електронний документообіг». Ускладнена процедура подачі в суд цього засобу доведення ставить під сумнів доцільність закріплення ст. 6 та ст. 7 цього Закону щодо наявності електронного цифрового підпису (далі – ЕЦП) обов'язковою вимогою для електронних документів [2]. Якщо ми розглядаємо фото та відеофіксацію як «електронний документ», то накладання електронного підпису для завершення створення цього доказу як такого стає майже неможливим. Не кожен ІТ-спеціаліст володіє знаннями відносно такої процедури. З одного боку, така норма регламентує достовірність та справжність таких доказів, а з іншого – обтяжує та затягує судочинство.

Для порівняння, відповідно до ч. 1 ст. 99 Кодексу адміністративного судочинства України електронними доказами є інформація в електронній (цифровій) формі, що містить відомості про

обставини, що мають значення для справи, в тому числі: електронні документи (текстові документи, графічні зображення, плани, фотографії, відео- і аудіозаписи); веб-сайти і сторінки; текстові, мультимедійні повідомлення; 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) [3].

Слід звернути увагу саме на ч.2 і ч.3 ст.99 Кодексу адміністративного судочинства України (далі - КАС України), відповідно до яких електронні докази подаються в оригіналі або в електронній копії, засвідченої ЕЦП. Учасники справи мають право подавати електронні докази на паперових носіях в порядку, визначеному законом. Паперова копія електронного доказу не є письмовим доказом. Тобто, роздруковане фото будь-якого документа, складеного в електронному вигляді, є паперовою копією електронного документа, але не як не письмовим доказом. Крім цього, згідно ч.4 ст.99 КАС України, учасник справи, який подає копію електронного доказу, повинен вказати про наявність у нього або у іншої особи оригіналу такого електронного доказу. В іншому випадку, якщо проігнорувати ці вимоги, тоді в позові буде вважатися порушенням вимог ст. 160 КАС України, у наслідок чого залишення позовної заяви без руху відповідно до ч. 1 ст. 169 КАС України. [4]

Якщо доцільно розглянути електронні докази як засіб протидії кіберзлочинності в кримінальному процесі, то тут з'являється більше питань, ніж відповідей.

Відповідно до глави 4, ст.84 Кримінального процесуального кодексу України (далі – КПК України) доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку [5].

Звісно, прийняття КПК 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 [6].

Варто зазначити, що розробці концепції кібердоказів у вітчизняній науці кримінального процесу та криміналістики було недостатньо приділено уваги. Одною із таких причин можна вважати як брак технічної освіти та знань в ІТ-сфері у правознавців. Неможливо розробляти механізм протидії кіберзлочинам, якщо не розуміти як діятимуть потенціальні злочинці і як їх можна зупинити. Така транснаціональна кримінальна злочинність, що діє у кіберпросторі, несе приховану небезпеку.

Більш того, через несучасність та невідповідність часові кримінально-процесуальних норм, сьогодні ми продовжуємо використовувати тлумачення законодавців в ЦПК України та КАС України щодо електронних доказів.

В умовах ІТ-глобалізації позитивно впливає на національне правотворення досвід країн Європейського союзу та США, де за допомогою прецедентного права визначають процес збирання доказів (зокрема, електронних).

Наприклад, у кримінальному судочинстві США відповідно до прецедентної судової практики, доказами визнавались аудіо- та відеозапис, фотографія, електронний документ, мобільний документ, текстові повідомлення, електронний носій інформації, портативний комп'ютер, електронна кореспонденція, дані інтернет-трафіку та ін. [7]

У Кримінально-процесуальному кодексі Республіки Молдова – аудіо- та відеозапис, фотографії та інші носії інформації є окремим різновидом матеріальних засобів доказування (ст. 164) [7].

У КПК Латвії є ст.136 «Електронні докази», відповідно до якої доказами в кримінальному процесі можуть бути відомості про факти у формі електронної інформації, обробленої збереженої або переданої пристроями або системами автоматизованої обробки даних [8].

Особливо слід привернути увагу саме на судову практику щодо використання як електронних доказів даних, розміщених у соціальних мережах та програмах для спілкування.

Завдяки всесвітньому поширенню електронних засобів комунікації (Viber, Skype, Telegram, WhatsApp, Messenger та ін.), з'явилася можливість вести з їх допомогою не тільки приватну переписку, але і направляти юридично значимі повідомлення.

Так, аналіз практики вирішення кримінальних, цивільних, господарських суперечок українськими, білоруськими та англійськими судами показує, що вони приймають листування в месенджерах як доказ у справі. Для того, щоб суд визнав листування в месенджері належним доказом, потрібно, щоб вона дозволяла встановити відправника, адресата, дату і час відправлення та інформацію про отримання. Тоді ця інформація можна буде розцінювати як допустимі і достовірні докази [9].

На прикладі справи визначеної судовою колегією в цивільних справах Мінського обласного суду від 15 січня 2018 року, суд розглянув справу про стягнення заробітної плати, компенсації за невикористану відпустку, середнього заробітку за затримку розрахунку. При цьому суд взяв до уваги листування між позивачкою та директором товариства з Viber в день звільнення позивачки. Директор погрожував їй звільненням за статтею і позовом до суду. У відповіді позивачка вимагала видати їй особову справу, трудову книжку і розрахунок, вказавши, що в іншому випадку сама звернеться до суду.

В іншій справі районного суду в Білорусі від 27 липня 2016 року, громадянка Х подала позов про визнання громадянки У такою, що втратила право користування житловим приміщенням. Суд своєчасно і в належній формі сповістив громадянку У по Viber про час і місце розгляду справи. У листуванні громадянка У пояснила причини неявки в судові засідання, що у подальшому стало матеріалом судової справи [9].

За вироком Подільського районного суду міста Києва, суд дослідивши скріншоти листування в Viber свідка з підсудної, встановив, що цим листуванням підтверджується домовленість про надання неправомірної вигоди для підозрюваної. Як підсумок, остання була засуджена за ст.368 Кримінального кодексу України, а саме «Прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою» [10].

Однак є і негативний досвід застосування електронних засобів комунікації. Не так давно детективам Національного антикорупційного бюро України була потрібна інформація Viber-листування одного з членів правління Одеського припортового заводу. Згідно з позицією НАБУ, «це листування в Viber може свідчити про причетність до переказу грошових коштів та їх подальшу конвертацію». Бюро планувало використати листування як доказ у кримінальному провадженні. Втім, суд в цьому клопотанні детективам відмовив [10].

З практики Печерського районного суду міста Києва від 22.05.2017 року про здійснення приводу свідка, суд взяв до уваги, що повістка про виклик свідка для його допиту в рамках кримінального провадження була направлена за допомогою повідомлення в Viber. Для підтвердження цього факту судді, слідчим було складено відповідний рапорт і надані скріншоти з месенджера. При цьому, статтею 135 КПК України не передбачено виклику особи до слідчого, прокурора або слідчого судді шляхом повідомлення на мобільний, в тому числі і на месенджери [10].

На прикладі судової практики країн ЄС, у Великобританії була гучна справа щодо жінки, що стверджувала про зґвалтування. Проте, дослідивши її мобільний телефон, було знайдено приватні повідомлення, що статеві відносини були обопільні [11].

Підбиваючи підсумки, можна стверджувати про особливу необхідність термінових змін в сучасному кримінальному процесі України. Саме невизначеність електронних доказів в законодавстві нашої країни призводить до загрози інформаційній безпеці наших громадян та робить нас вразливими до особливої групи кримінальних правопорушень – кіберзлочинів. Слід уважно дослідити нормативно-правову базу інших галузей процесуального вітчизняного та зарубіжного права, а також детально приділити вагу судовій практиці щодо використання електронних доказів задля коректної та ефективної регламентації в сучасному кримінальному процесі.

Список бібліографічних посилань

1. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40-41, 42. Ст.492.
2. Зоуля Н. Недієвість процедури подання електронних доказів у цивільному процесі // Українське право. 05.06.2018 10:00. URL: <http://ukrainepravo.com/scientific-thought/naukova-dumka/nediyevist-protsedury-podannya-elektronnykh-dokaziv-u-tsyvilnomu-protsesi/> (дата звернення: 31.10.2018).
3. Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV. *Відомості Верховної Ради України*. 2005. № 35-36, № 37. Ст. 446.
4. Гольдарб Я. Ю. Электронные доказательства в административном процессе // Протокол: юридичний інтернет-ресурс. 11.01.2018. URL: https://protocol.ua/ua/elektronnie_dokazatelstva_v_administrativnom_protseesse/ (дата звернення: 31.10.2018).
5. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України*. 2013. № 9-10, № 11-12, № 13. Ст. 88.
6. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія право*. 2016. Випуск 36. Том 2. С. 123-125. URL: http://www.visnyk-juris.uzhnu.uz.ua/file/No.36/part_2/32.pdf (дата звернення: 31.10.2018).
7. Сергеев М. С. Электронные доказательства в уголовном судопроизводстве. Опыт США. *Вестник экономики, права и социологии. Серия право*. 2016. № 2. С. 206-214.
8. Уголовно-процессуальный закон : Закон, принятый Сеймом 21 апреля 2005 года и обнародованный Президентом государства 11 мая 2005 года (с изменениями, внесенными по состоянию на 28 сентября 2005 года) // Законы Латвии по-русски. URL: http://www.pravo.lv/likumi/29_upz.html (дата звернення: 31.10.2018).
9. Бандык О. Переписка в мессенджере как средство доказывания в суде // Плех-новости. 21.09.2018. URL: <https://ilex.by/perepiska-v-messendzhere-kak-sredstvo-dokazyvaniya-v-sude/> (дата звернення: 31.10.2018).
10. Довбыш Р. Как переписка в мессенджерах может привести вас в зал судебного заседания в роли ответчика // Украина криминальная. 29 ноября 2017. URL: <http://cripo.com.ua/likbez/?p=239399/> (дата звернення: 31.10.2018).
11. Bowcott Owen, Justice system at 'breaking point' over digital evidence // The Guardian, Mon 12 Feb 2018 06:00. URL: <https://www.theguardian.com/law/2018/feb/12/justice-system-at-breaking-point-over-digital-evidence> (дата звернення: 31.10.2018).

Одержано 02.11.2018