DOI: 10.31359/2079-6242-2022-46-32
УДК 343.98

Г. К. Авдєєва, кандидат юридичних наук, старший науковий співробітник, провідний науковий співробітник Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України

ЦИФРОВІ ДОКАЗИ І СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВОЗАСТОСОВНІЙ ДІЯЛЬНОСТІ

Постановка проблеми. Наприкінці XX століття завдяки розвитку цифрових і мережевих технології у правозастосовній діяльності розпочалася робота з інформацією у цифровій формі, яка містилася в електронних пристроях (мобільних телефонах, комп'ютерах, фото- та відеокамерах, GPS-навігаторах) та телекомунікаційних мережах (у соціальних мережах, на різних сайтах у мережі Інтернет та ін.). Поява нових поколінь електронних пристроїв та програмних продуктів призвели до виникнення нових типів сигналів і форматів даних, збільшення кількості способів кодування і перетворення інформації у цифровому вигляді. За допомогою звичайної комп'ютерної техніки зі стандартним програмним забезпеченням на сьогодні вже неможливо переглянути і дослідити окремі види інформації (наприклад, записи бортових реєстраторів літальних апаратів). Для цього необхідні спеціальні електронні пристрої і спеціальне програмне забезпечення. Це викликає певні труднощі у суддів, слідчих, прокурорів, адвокатів, судових експертів при дослідженні й оцінці цифрових доказів.

При розслідуванні воєнних злочинів набули актуальності проблеми встановлення допустимості цифрових доказів у кримінальному провадженні. Найчастіше цифрові аудіо- та відеозаписи, на яких міститься інформація про протиправну діяльність військових рф, здійснювалися задовго до відкриття кримінального провадження і, зрозуміло, слідчий не мав можливості зафіксувати її у процесуальних актах.

За даними Офісу Генерального прокурора, станом на жовтень 2023 р. зафіксовано інформацію щодо понад 100 тис. таких злочинів[1], яка разом з іншими доказами дозволить не лише довести факт вчинення злочину, а й встановити конкретних осіб-злочинців, висунути їм обґрунтоване обвинувачення та притягнути до кримінальної відповідальності. Однак судді і слідчі часто мають певні труднощі в оцінці цифрових доказів через відсутність у законодавстві України їх визначення, порядку фіксації та оцінки. Через це цифрові докази судами України іноді не визнаються допустимими, а рекомендації науковців щодо цих питань у галузі права ЄС та США найчастіше використовуються лише журналістами-розслідувачами[2]. Тобто законодавство України не встигає за стрімким розвитком інформаційних технологій, а прогалини правого регулювання часто доводиться заповнювати судовою практикою.

Різновидом цифрових технологій є системи штучного інтелекту (ШІ). Вони активно використовуються в промисловості, медицині, транспорті, сільському господарстві, науці й освіті, побуті, системах комунікації, військовій справі. На сьогодні єдиного загальновизнаного визначення цього терміна не існує, оскільки це міждисциплінарна наука, яка поєднує багато галузей (інформатика, математика, соціологія, психологія, право та ін.). У загальному розумінні системами ШІ є комп'ютерні системи, що не лише виконують певні завдання за заздалегідь заданим алгоритмом, а й вирішують творчі завдання на основі аналізу значної за обсягом різноманітної інформації та імітують такі процеси мислення людини, як навчання,

[1] 'Офіс Генерального прокурора' <https://gp.gov.ua/> (дата звернення: 01.11.2023).

[2] Авдєєва Г., Живуцька-Козловська Е. 'Проблеми використання цифрових доказів у кримінальному судочинстві України та США' (2023) 1 Теорія та практика судової експертизи і криміналістики : зб. наук. пр. 128 <https://doi.org/10.32353/khrife.3.2022.08> 128

прогнозування, оцінка ризиків, робота з неповними даними та ін. [1]

У правозастосовній діяльності системи ШІ також показали свою ефективність. Зокрема, системи безпеки дорожнього руху з елементами ШІ допомагають збирати доказову інформацію при розслідуванні дорожньо-транспортних подій. Вони виявляють порушення правил дорожнього руху, допомагають ідентифікувати транспортні засоби та осіб в несприятливих умовах (низька роздільна здатність фото- або відеокамери, темрява, снігопад, дощ тощо)[2].

Незважаючи на активне використання цифрових доказів і систем ШІ в правозастосовній діяльності, визначення їх понять у законодавстві України відсутнє. Так само не визначено види ШІ, принципи їх використання, межі, умови, порядок застосування тощо. До того ж є відсутньою регламентація процесів збирання, фіксації та оцінки цифрових доказів. Ці питання є вкрай актуальними і мають досліджуватись науковцями.

Аналіз останніх досліджень і публікацій. Окремі проблеми використання електронних (цифрових) доказів у кримінальному судочинстві висвітлені у роботах таких вітчизняних та закордонних вчених: Ю. Орлов, М. Гуцалюк, С. Столітній, Д. Цехан, В. Шевчук, В. Шепітько, Шон Е. Гудісон[3], П. Левуліс[4], Мартін Новак[5] та ін.

Проблеми визначення напрямів використання ШІ у правозастосовній діяльності і їх правового регулювання досліджувались багатьма вітчизняними і закордонними дослідниками, такими як: М. Карчевський, В. Шевчук, О. Радутний, Т. Шевчук, Дж. Сартора (1998)[6], К. Рігано (2019)[7], А. Іддер (2021)[8], Алі Ф. Кабола (2022)[9] та ін.

Незважаючи на значну кількість публікацій щодо проблем використання цифрових доказів і систем ШІ у правозастосовній діяльності, окремі питання потребують подальшого дослідження. Зокрема, невирішеними залишаються проблеми законодавчого закріплення поняття «цифровий доказ», а також – окремі проблеми процесуальної регламентації їх вилучення, фіксації, зберігання і оцінки. Актуальними є й проблеми правового регулювання процесів використання ШІ в Україні та за її межами, пошуки нових напрямів застосування систем ШІ у правозастосовній діяльності, визначення меж використання систем ШІ з метою захисту прав людини, тощо. Зазначені питання викликають численні дискусії і на сьогодні ще не вироблені чіткі позиції щодо їх вирішення.

Метою статті є аналіз співвідношення понять «електронний доказ та «цифровий доказ», уточнення поняття «цифровий доказ», узагальнення судової практики України з метою виокремлення проблем, які виникають під час використання цифрових доказів у кримінальному судочинстві, та надання пропозицій щодо вдосконалення кримінального процесуального законодавства України у частині досліджуваних проблем; установлення ролі технологій ШІ у правозастосовній діяльності в Україні; аналіз обмежень у їх застосуванні; визначення перспективних напрямів використання систем ШІ у правозастосовній діяльності; виокремлення невирішених правових проблем, із цим пов'язаних.

---

[1] Авдєєва Г. К. 'Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції' *Використання технологій штучного інтелекту у протидії злочинності : матеріали наук.-практ. онлайн-семінару* (5 листоп. 2020 р.) 6

[2] Авдєєва Г. К. 'Проблеми використання систем штучного інтелекту у правозастосовній діяльності' (2023) 2 Вісник ЛДУВС ім. Е. О. Дідоренка 65 <DOI:10.33766/2524–0323.102.63–80> (дата звернення: 01.11.2023).

[3] Sean E. Goodison; Robert C. Davis; Brian A. Jackson. 'Digital Evidence and the U. S. Criminal Justice System – Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence' National Institute of Justice <https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf> (дата звернення: 02.11.2023).

[4] Lewulis, P. Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law. (2022) Crim Law Forum 33, 39–62 <https://doi.org/10.1007/s10609-021-09430-4> (дата звернення: 04.11.2023).

[5] Novak, Martin 'Digital Evidence in Criminal Cases Before the U. S. Courts of Appeal: Trends and Issues for Consideration' (2020) 14 (4) Journal of Digital Forensics, Security and Law DOI: https://doi.org/10.15394/jdfsl.2019.1609 (дата звернення: 01.11.2023).

[6] Sartor, G., Branting, L. K. *Introduction: Judicial Applications of Artificial Intelligence*. Judicial Applications of Artificial Intelligence. (Springer, Dordrecht, 1998).. DOI : https://doi.org/10.1007/978-94-015-9010-5_1 (дата звернення: 03.11.2023).

[7] Christopher Rigano 'Using Artificial Intelligence to Address Cri minal Justice Needs' (2019) January NIJ Journal 280 <https://www.nij.gov/journals/ 280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.Aspx> (дата звернення: 02.11.2023).

[8] Asma Idder, Stephane Coulaux. 'Artificial intelligence in criminal justice: invasion or revolution?' (International Bar Association, 13 December 2021) <https://www.ibanet.org/dec-21-ai-criminal-justice> (дата звернення: 03.11.2023).

[9] Ali Faghiri Kabol 'The Use Of Artificial Intelligence In The Criminal Justice System' (A Comparative Study). Article in Webology November 2022. <https:// www.researchgate.net/publication/365027297_The_Use_Of_Artificial_Intelligence_In_The_Criminal_Justice_System_A_Comparative_Study> (дата звернення: 01.11.2023).

Виклад основного матеріалу. Науковці у галузі кримінально-правових наук використовують терміни «електронні» та «цифрові» докази як рівнозначні, але між ними існують такі відмінності: аналогова інформація є безперервною, а цифрова – дискретною. На сьогодні цифрові пристрої повністю витіснили аналогові.

Термін «цифровий доказ» є більш точним для інформації у цифровій формі та краще віддзеркалює кібернетичний аспект передачі, обробки та збереження інформації за допомогою бінарного (двійкового) коду. Однак слід ураховувати, що доказами є фактичні дані, отримані з належних джерел, а їх матеріальною основою слугує вже не саме джерело, а штучно створений відповідний процесуальний носій. При цьому доказ являє собою єдність фактичних даних та їх процесуальних носіїв[1]. Тому термін «електронний доказ» також має право на існування, оскільки він може бути пристроєм, який створює, обробляє або зберігає інформацію у цифровій формі.

Д. Цехан під «цифровими доказами» розуміє «фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для сприйняття людиною»[2]. Це визначення потребує уточнення. Зокрема, не всі носії здатні зберігати інформацію у цифровій формі (зокрема, папір і магнітна плівка також є носіями інформації). Також для розшифровування і дослідження деяких видів цифрової інформації потрібні не ЕОМ, а спеціальні електронні прилади зі спеціальним програмним забезпеченням (наприклад, для перегляду записів спеціальних програмно-апаратних засобів з унікальною файловою системою). Тому цифровими доказами слід вважати фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення справи.

На відміну від Цивільного процесуального кодексу України (ст. 100)[3], Господарського процесуального кодексу України (ст. 96)[4] та Кодексу адміністративного судочинства України (ст. 99)[5] у Кримінальному процесуальному кодексі України (КПК) відсутні положення про електронні (цифрові) докази. Інформацію у цифровій формі у КПК віднесено до документів/електронних документів як процесуальних джерел доказів (ч.2 ст. 84 КПК)[6]. До документів віднесено також «матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані)» (п. 1 ч. 2 ст. 99 КПК) та «носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії» (п. 3 ч. 2 ст. 99 КПК). При цьому оригіналом електронного документа зазначено «його відображення, якому надається таке саме значення, як документу» (ч. 3 ст. 99 КПК). Дублікати документів та копії інформації у цифровій формі, виготовлені «слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа» (ч. 4 ст. 99 КПК). В абз. 2 ч. 2 ст. 237 КПК регламентовано огляд комп'ютерних даних, але там бракує обов'язкового переліку інформації щодо порядку фіксації цифрових доказів.

Документами як цифровими доказами можуть слугувати не лише текстові документи, малюнки, фотознімки, аудіо- та відеозаписи, а й комп'ютерні програми та бази даних. Вони відрізняються не лише за формою та змістом, а й за джерелом походження. Електронні документи, в основному, створює людина, інші докази в цифровій формі виникають унаслідок роботи електронних пристроїв і систем та не залежать від дій людини (інформація з навігаційно-моніторингових систем, електронний цифровий підпис, мережева технологічна інформація тощо). Такі цифрові докази за своєю сутністю не можуть бути віднесені до документів і їх використання у правозастосовній діяльності потребує окремого законодавчого врегулювання.

На відміну від України, у країнах ЄС, США та, зокрема, в Міжнародному кримінальному суді ви-

---

[1] Тертишник В. М. *Кримінальний процес України. Загальна частина: підручник* (Київ: Алерта, 2014) 288

[2] Цехан Д. М. 'Поняття електронних (цифрових) доказів у кримінальному провадженні та їх види' *Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник* (Львів : ЛНУ ім. Івана Франка, 2022) 133

[3] Цивільний процесуальний кодекс України від 18.03.2004 р. №1618-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1618–15#Text (дата звернення: 02.11.2023).

[4] Господарський процесуальний кодекс України від 06.11.1991 р. №1798-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1798–12#Text (дата звернення: 02.11.2023).

[5] Кодекс адміністративного судочинства України від 06.07.2005 р. №2747-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2747–15#Text (дата звернення: 02.11.2023).

[6] Кримінальний процесуальний кодекс України від 13.04.2012 р. №4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text (дата звернення: 02.11.2023).

користання цифрових доказів регулюється багатьма нормами процесуального законодавства. Їх основою слугують принципи роботи з цифровими доказами, викладені у міжнародному стандарті ISO/IEC 27037:2012[1], Протоколі Берклі[2], матеріалах міжнародної Наукової робочої групи з цифрових доказів (SWGDE)[3], Керівних принципах Комітету Міністрів Ради Європи щодо електронних доказів у цивільних та адміністративних провадженнях[4], Федеральних правилах доказування (FRE, США)[5] та ін.

Аналіз понад 50 ухвал, рішень і постанов Верховного Суду, рішень місцевих судів м. Харкова і Харківської області, рішень Апеляційного суду Харківської області та Харківського апеляційного суду, в яких здійснювались дослідження й оцінка цифрових доказів, показав, що під час розгляду справ у судах різних юрисдикцій виникають певні труднощі щодо визнання інформації у цифровій формі допустимими і достовірними доказами. За однакових умов судді іноді навіть приймали протилежні рішення.[6] В одних випадках вони визнавали копії цифрових записів допустимими доказами, в інших – недопустимими (особливо щодо корупційних злочинів). Як наслідок, не визнавалися допустимими доказами і судові експертизи, в яких досліджувались цифрові докази.

Часто суди покладаються на клопотання адвокатів про недопустимість цифрового доказу через те, що спочатку з телефона або іншого пристрою інформація копіювалася на комп'ютер, а лише згодом – на оптичний диск або флешнакопичувач, який потім надавався слідчому (суду) як процесуальний носій доказу. Захисники вважають, що така копія не відповідає оригіналу тому, що при зміні носіїв інформації змінюється формат файлу. Це є хибним твердженням тому, що однією з основних ознак інформації у цифровій формі є те, що всі її копії, зафіксовані на різних носіях, є ідентичними оригіналу (повністю співпадають за всіма ознаками, включаючи формат файлу).

Аналіз вітчизняних та закордонних публікацій показав, що від компетенції співробітників правозастосовних органів (слідчих, суддів, прокурорів, оперативних працівників, судових експертів) та наявності відповідних науково-методичних рекомендацій щодо роботи з інформацією у цифровій формі залежить, чи буде окремий цифровий доказ відігравати провідну роль у вирішенні конкретної справи. Помилки, яких у процесі отримання доказів припускаються суб'єкти розслідування злочинів, можуть спричинити втрату значної частини доказів на етапі судового розгляду, якщо суд визнає такі докази недопустимими через порушення процесуальних норм під час їх збирання[7]. Вони повинні знати базові технічні характеристики цифрових пристроїв і цифрової інформації та правила її фіксації. Відповідна методична і довідкова література має бути розроблена і включена до програм підвищення кваліфікації окремо для кожної категорії співробітників[8].

Системи ШІ як один із видів цифрових тезнологій показали свою ефективність у правозастосовній діяльності. Зокрема, в Апараті РНБО України використовується сучасна багатофункціональна інформаційно-аналітична система з елементами

---

[1] ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html (дата звернення: 07.02.2023).

[2] *Примітка.* Протокол Берклі – рекомендаційний документ, який у 2020 році представили Центр прав людини Університету Берклі в Каліфорнії та Офіс Верховного комісара ООН з прав людини. Він окреслює мінімальні стандарти для пошуку, збирання, зберігання, перевірки та аналізу відкритих джерел, і може слугувати практичним посібником для адвокатів, журналістів та дослідників. На практиці Протоколом Берклі уже зараз керуються Офіс Генерального прокурора разом з українськими та міжнародними партнерами під час збору доказів про воєнні злочини РФ.

[3] Positions and Considerations of Scientific Working Group on Digital Evidence. URL: https://www.swgde.org/documents/positions-and-considerations (дата звернення: 04.11.2023).

[4] Керівні принципи Комітету Міністрів Ради Європи CM(2018)169-add1final щодо електронних доказів у цивільних та адміністративних провадженнях. Міністерство юстиції України: офіційний сайт. URL: https://minjust.gov.ua/m/rekomendatsii-parlamentskoi-asamblei-ta-komitetu-ministriv-radi-evropi (дата звернення: 03.11.2023).

[5] Federal Rules of Evidence (FRE), as amended to December 1, 2020. Legal Informational Institute. URL: https://www.law.cornell.edu/rules/fre (дата звернення: 01.11.2023).

[6] Ухвала ВС від 29.05.2018 р. Справа №397/2588/13-к. Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/74475933; Постанова ВС від 15.01.2020 р. Справа №161/5306/16-к. Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/Review/87053591 (дата звернення: 01.11.2023).

[7] Брендель, О., Нікулін, К., Асланова, Е. 'Можливості експертизи відео-, звукозапису під час розслідування злочинів, пов'язаних із торгівлею людьми' (2022) 2 (27) Теорія та практика судової експертизи і криміналістики 140 DOI: 10.32353/khrife.2.2022.10

[8] Авдєєва Г. 'Проблеми визнання цифрових відеозаписів, отриманих під час відеоконтролю особи, допустимими доказами' *Актуальні проблеми правоохоронної діяльності в умовах воєнного стану* : *тези Всеукраїнської науково-практичної конференції* (Хмельницький, 16 березня 2023 року) 543–544

ШІ «СОТА»[1], яка слугує інструментом аналізу та управління ризиками у сфері національної безпеки та оборони України.

Міністерство юстиції України до Єдиного реєстру засуджених осіб підключило аналітичну систему з елементами ШІ «Касандра», яка аналізує різноманітну інформацію про засуджених осіб та виявляє ризики повторного кримінального правопорушення.

Система ШІ ePOOLICE (early Pursuit against Organized crime using environmental scanning, the Law and Intelligence systems) з 2013 р. успішно використовується в країнах-членах ЄС. Вона аналізує сторінки сайтів, електронне листування, поліцейську інформацію для пошуку інформації про діяльність організованих злочинних груп та здійснює оцінку ризику появи кримінальної активності [2].

У Великій Британії система штучного інтелекту HART (Harm Assessment Risk Tool) показала свою ефективність при прогнозуванні появи ризику рецидиву злочину щодо раніше засуджених осіб.

У Сполучених Штатах Америки для оцінки ймовірності скоєння підсудним рецидиву злочину та аналізу попередніх проступків використовуються такі системи ШІ: Watson/Ross – IBM (аналітика), COMPAS – Correctional Offender Management Profiling for Alternative та ін.

Системи ШІ у різних країнах світу використовуються під час розслідування злочинів для отримання інформації про осіб та їх дії, різноманітні об'єкти і явища з метою виявлення і попередження шахрайських дій, для ідентифікації осіб і предметів (у т. ч. зброї) за їх слідами та ін.

При розслідуванні воєнних злочинів, учинених військовослужбовцями рф в Україні, системи ШІ ефективно вирішують завдання щодо ідентифікації осіб за фотознімками, відеозаписами та пробами ДНК. Зокрема, за допомогою американської системи розпізнавання осіб Clearview AI, яка використовує базу даних із 30 млрд фотопортретів із соціальних мереж та стрічок новин, встановлено особи окремих злочинців-військовослужбовців рф за їх фотознімками[3].

Науковці у галузі кримінального права активно дискутують щодо можливості визнання систем ШІ суб'єктами правовідносин. Зокрема, О. Радутний вважає ШІ електронною особою (особистістю) та рекомендує застосовувати до нього заходи кримінально-правового характеру[4]. Т. Каткова пропонує внести зміни в кримінальне законодавство з метою визначення кримінальної відповідальності ШІ[5]. В. Грига вважає можливим навіть визнавати ШІ потерпілим від злочину[6]. З такими пропозиціями погодитися не можна, особливо в разі настання цивільно-правової відповідальності. Досвідчений фахівець Аналітичного центру з міжнародного розвитку в галузі кібербезпеки Пабло Лазаро справедливо зазначає, що «робот не може нести відповідальність за дії або бездіяльність, які можуть завдати шкоди третім особам. Судді судять людей, а не роботів, не кажучи вже про алгоритми». [7]

Попри ефективну роботу з великими масивами інформації, системи ШІ мають і певні недоліки. Науковці попереджають, що важливо враховувати законодавчі обмеження щодо застосування штучного інтелекту в розслідуванні злочинів, зокрема, заборони на використання деяких видів даних, які можуть порушувати права людини[8]. Тобто стрімкий розвиток і широке розповсюдження систем ШІ випереджають процеси створення умов і засобів ефективної протидії недоброчесному і зловмисному їх використанню.

Для отримання якісного законодавства, яке регулюватиме порядок використання ШІ у правозастосовній діяльності, до його розробки мають

[1] 'В Апараті РНБО України розроблено та введено в експлуатацію сучасну інформаційно-аналітичну систему «СОТА».' (РНБО: офіційний сайт) <https://www.rnbo.gov.ua/ua/Diialnist/5011.html> (дата звернення: 03.11.2023).

[2] 'Early Pursuit against Organized crime using envirOnmental scanning, the Law and IntelligenCE systems' (European Commission)<https://cordis.europa.eu/project/id/312651> (дата звернення: 03.11.2023).

[3] Джеймс Клейтон. 'Як штучний інтелект допомагає ідентифікувати загиблих в Україні' (BBC News Україна) <https://www.bbc.com/ukrainian/features-61105661> (дата звернення: 03.11.2023).

[4] Радутний О. Є. 'Кримінальна відповідальність штучного інтелекту' (2017) 2(21) Інформація і право 131

[5] Каткова Т. 'Штучний інтелект в Україні: правові аспекти' (2020) 6 Право і суспільство 53

[6] Грига В. 'Штучний інтелект як потерпілий від злочину' (2019) 5(69) Молодий вчений 191

[7] Pablo Lázaro 'Artificial Intelligence in Criminal Investigation. Agenda for International Development' (A-id) <https://www.a-id.org/artificial-intellige nce-in-criminal-investigation> (дата звернення: 04.11.2023).

[8] Baltrūnienė J., Shevchuk V. 'Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience' *Цифрова трансформація кримінального провадження в умовах воєнного стану* : *мат-ли Всеукр. круглого столу* (Харків, 16.12.2022) 139

долучатися науковці в галузі права, судді, слідчі, адвокати та інші співробітники правозастосовної сфери.

Висновки. У кримінальному процесуальному законодавстві України не лише відсутнє визначення терміна «цифрові докази», а й не зазначений порядок їх збирання, зберігання, аналізу та використання у кримінальному провадженні. Тому КПК України бажано доповнити такими новелами: визначення поняття цифрових доказів та їх процесуальних носіїв; розмежування понять «електронний доказ» і «цифровий доказ»; докладний порядок вилучення цифрової інформації, її огляду, фіксації і зберігання із зазначенням переліку обов'язкової інформації щодо цифрових доказів, яка має бути процесуально закріплена; порядок оцінки допустимості і достовірності цифрового доказу за певними критеріями.

Перспективними завданнями щодо розробки систем ШІ в Україні для потреб правозастосовних органів є такі: вивчення соціальних мереж і сайтів, поліцейської інформації для пошуку відомостей про діяльність організованих злочинних груп із метою оцінки ризику появи кримінальної активності; прогнозування ступеню ризику рецидиву злочину щодо раніше засуджених осіб; виявлення неправдивої інформації в мережі Інтернет та встановлення її джерел, пошук у відкритому доступі та аналіз потенційних джерел доказів – величезної кількості загальнодоступних відео- та аудіозаписів, фото та супутникових знімків, текстів, звітів, публікацій у соціальних мережах; отримання інформації про певних осіб та їх дії, а також про зв'язки між певними особами шляхом моніторингу відкритих джерел; виявлення потенційних свідків злочинів шляхом аналізу інформації, яка міститься в мережі Інтернет; дослідження інформації, яка міститься в мобільному телефоні та інших електронних пристроях із метою виявлення фактів і часу здійснення і приймання дзвінків, певних контактів, фотознімків, відео- та звукозаписів, текстових файлів і повідомлень, електронних листів, інформації в соціальних мережах, месенджерах і сервісах спілкування та ін. для її систематизації за певними критеріями та формування звітів за певними запитами (із дотриманням прав людини та з урахуванням захисту персональних даних); ідентифікація осіб за фотознімками, відеозаписами, текстами, голосом, ДНК; встановлення виду взуття, транспортного засобу, знаряддя або інструменту, зброї та ін. та ідентифікація цих об'єктів за їх слідами, залишеними на місці події; встановлення аутентичності (справжності, достовірності) цифрових відео- та аудіозаписів тощо.

В Україні доцільно прийняти єдиний нормативно-правовий акт у формі закону, який розв'язав би всі можливі проблеми використання ШІ у правозастосовній діяльності. Особливу увагу слід приділити визначенню меж використання систем ШІ, які мають відповідати таким принципам: дотримання прав людини; об'єктивність і точність результатів аналізу інформації; компетентність розробників ШІ та уповноважених осіб, які його використовують; підзвітність; відповідність законодавству; безпека збереження інформації та електронних пристроїв; запобігання будь-якій дискримінації між окремими особами чи групами осіб; якість та безпека при обробленні процесуальних рішень і даних, які мають міститися у безпечному технологічному середовищі; незалежність, прозорість, неупередженість, справедливість та ін. Слід враховувати, що процедура доказування у процесуальній діяльності являє собою всебічний аналіз і зіставлення лише об'єктивної доказової інформації. Вона відрізняється від автоматичного аналізу даних системою ШІ, який може враховувати недостовірні або підроблені дані, неправдиві показання свідка або потерпілого, помилкові висновки експерта та ін. Це може вплинути на правильність висновку штучного інтелекту і призвести до порушення таких фундаментальних принципів судочинства, як верховенство права, недискримінація, неупередженість, справедливість та ін. Тому системи ШІ можуть слугувати лише допоміжним інструментом уповноважених осіб під час прийняття процесуальних рішень. Повністю автоматизувати ці процеси в Україні поки що зарано.

REFERENCES

List of legal documents

Legislation

1. Tsyvilnyi protsesualnyi kodeks Ukrainy vid 18.03.2004 r. № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618–15#Text (in Ukrainian)

2. Hospodarskyi protsesualnyi kodeks Ukrainy vid 06.11.1991 r. №1798-XII. URL: https://zakon.rada.gov.ua/laws/show/1798–12#Text (in Ukrainian)
3. Kodeks administratyvnoho sudochynstva Ukrainy vid 06.07.2005 r. №2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747–15#Text (in Ukrainian)
4. Kryminalnyi protsesualnyi kodeks Ukrainy vid 13.04.2012 r. №4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text (in Ukrainian)
5. Federal Rules of Evidence (FRE), as amended to December 1, 2020. Legal Informational Institute. URL: https://www.law.cornell.edu/rules/fre (in English)
6. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html (in English)
7. Positions and Considerations of Scientific Working Group on Digital Evidence. URL: https://www.swgde.org/documents/positions-and-considerations (in English)
8. Kerivni pryntsypy Komitetu Ministriv Rady Yevropy CM(2018)169-add1final shchodo elektronnykh dokaziv u tsyvilnykh ta administratyvnykh provadzhenniakh. Ministerstvo yustytsii Ukrainy: ofitsiinyi sait. URL: https://minjust.gov.ua/m/rekomendatsii-parlamentskoi-asamblei-ta-komitetu-ministriv-radi-evropi (in Ukrainian)
9. Ukhvala VS vid 29.05.2018 r. Sprava №397/2588/13-k. Yedynyi derzhavnyi reiestr sudovykh rishen. URL: http://reyestr.court.gov.ua/Review/74475933 (in Ukrainian)
10. Postanova VS vid 15.01.2020 r. Sprava №161/5306/16-k. Yedynyi derzhavnyi reiestr sudovykh rishen. URL: http://www.reyestr.court.gov.ua/Review/87053591 (in Ukrainian)

Bibliography

Authored books

1. Tertyshnyk V. M. *Kryminalnyi protses Ukrainy. Zahalna chastyna: pidruchnyk* [Criminal process of Ukraine. General part: textbook] (Kyiv: Alerta, 2014) 288 (in Ukrainian)
2. Tsekhan D. M. *Poniattia elektronnykh (tsyfrovykh) dokaziv u kryminalnomu provadzhenni ta yikh vydy* [The concept of electronic (digital) evidence in criminal proceedings and their types] Kiberzlochynnist ta elektronni dokazy = Cybercrime and digital evidence : navch. posibnyk (Lviv : LNU im. Ivana Franka, 2022) 133 (in Ukrainian)

Edited books

3. Sartor, G., Branting, L. K.. *Introduction: Judicial Applications of Artificial Intelligence*. Judicial Applications of Artificial Intelligence. (Springer, Dordrecht, 1998) DOI : https://doi.org/10.1007/978-94-015-9010-5_1 (in English)

Journal articles

4. Avdieieva H., Zhyvutska-Kozlovska E. ’Problemy vykorystannia tsyfrovykh dokaziv u kryminalnomu sudochynstvi Ukrainy ta SShA’ [Problems of using digital evidence in criminal justice in Ukraine and the USA] (2023) 1 Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky : zb. nauk. pr. 128 https://doi.org/10.32353/khrife.3.2022.08 128 (in Ukrainian)
5. Avdieieva H. K. ’Problemy vykorystannia system shtuchnoho intelektu u pravozastosovnii diialnosti’ [Problems of using artificial intelligence systems in law enforcement activities] (2023) 2 Visnyk LDUVS im. E. O. Didorenka 65. DOI:10.33766/2524–0323.102.63–80 (in Ukrainian)
6. Sean E. Goodison; Robert C. Davis; Brian A. Jackson. ’Digital Evidence and the U. S. Criminal Justice System – Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence’ <https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf> (in English)
7. Lewulis, P. ’Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law’ (2022) Crim Law Forum 39–62 <https://doi.org/10.1007/s10609-021-09430-4> (in English)
8. Novak, Martin ’Digital Evidence in Criminal Cases Before the U. S. Courts of Appeal: Trends and Issues for Consideration’ (2020) 14 (4) Journal of Digital Forensics, Security and Law DOI: https://doi.org/10.15394/jdfsl.2019.1609 Available at: (in English)
9. Christopher Rigano ’Using Artificial Intelligence to Address Cri minal Justice Needs’ (2019) January NIJ Journal 280 <https://www.nij.gov/journals/ 280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.Aspx> (in English)
10. Brendel, O., Nikulin, K., Aslanova, E. ’Mozhlyvosti ekspertyzy video-, zvukozapysu pid chas rozsliduvannia zlochyniv, poviazanykh iz torhivleiu liudmy’ [Possibilities of examination of video and sound recordings during the investigation of crimes related to human trafficking] (2022) 2 (27) Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky 140 DOI: 10.32353/khrife.2.2022.10 (in Ukrainian)

11. Radutnyi O. Ye. 'Kryminalna vidpovidalnist shtuchnoho intelektu' [Criminal responsibility of artificial intelligence] (2017) 2(21) Informatsiia i pravo 131 (in Ukrainian)
12. Katkova T. 'Shtuchnyi intelekt v Ukraini: pravovi aspekty' [Artificial intelligence in Ukraine: legal aspects] (2020) 6 Pravo i suspilstvo 53 (in Ukrainian)
13. Hryha V. 'Shtuchnyi intelekt yak poterpilyi vid zlochynu' [Artificial intelligence as a victim of a crime] (2019) 5(69) Molodyi vchenyi 191 (in Ukrainian)

Conference paper

14. Avdieieva H. K. Problemy vykorystannia system shtuchnoho intelektu v roboti orhaniv kryminalnoi yustytsii [Problems of using artificial intelligence systems in the work of criminal justice bodies] *Vykorystannia tekhnolohii shtuchnoho intelektu u protydii zlochynnosti* : materialy nauk.-prakt. onlain-seminaru (5 lystop. 2020 p.) 6 (in Ukrainian)
15. Avdieieva H. Problemy vyznannia tsyfrovykh videozapysiv, otrymanykh pid chas videokontroliu osoby, dopustymymy dokazamy [Problems of recognizing digital video recordings obtained during video surveillance of a person as admissible evidence] *Aktualni problemy pravookhoronnoi diialnosti v umovakh voiennoho stanu* : tezy Vseukrainskoi naukovo-praktychnoi konferentsii (Khmelnytskyi, 16 bereznia 2023 roku) 543–544 (in Ukrainian)
16. Baltrūnienė J., Shevchuk V. 'Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience' *Tsyfrova transformatsiia kryminalnoho provadzhennia v umovakh voiennoho stanu* : mat-ly Vseukr. kruhloho stolu (Kharkiv, 16.12.2022) 139 (in English)

Websites

17. Ali Faghiri Kabol. 'The Use Of Artificial Intelligence In The Criminal Justice System (A Comparative Study)' (Article in Webology November 2022) <https:// www.researchgate.net/publication/365027297_The_Use_Of_Artificial_ Intelligence_ In_The_Criminal_Justice_System_A_Comparative_Study> (in English)
18. Asma Idder, Stephane Coulaux. 'Artificial intelligence in criminal justice: invasion or revolution?' (International Bar Association, 13 December 2021) <https://www.ibanet.org/dec-21-ai-criminal-justice> (in English)
19. 'Ofis Heneralnoho prokurora' (Ofitsiinyi sait) <https://gp.gov.ua/> (in Ukrainian)
20. 'V Aparati RNBO Ukrainy rozrobleno ta vvedeno v ekspluatatsiiu suchasnu informatsiino-analitychnu systemu «SOTA»' [In the apparatus of the National Security and Defense Council of Ukraine, a modern information and analytical system «SOTA» was developed and put into operation] (RNBO: ofitsiinyi sait) <https://www.rnbo.gov.ua/ua/Diialnist/5011.html> (in Ukrainian)
21. Dzheims Kleiton. 'Yak shtuchnyi intelekt dopomahaie identyfikuvaty zahyblykh v Ukraini' [How artificial intelligence helps to identify the dead in Ukraine] (BBC News Ukraina) <https://www.bbc.com/ukrainian/features-61105661> (in Ukrainian)
22. Pablo Lázaro 'Artificial Intelligence in Criminal Investigation' (Agenda for International Development) <https:// www.a-id.org/artificial-intellige nce-in-criminal-investigation> (in English)
23. 'Early Pursuit against Organized crime using envirOnmental scanning, the Law and IntelligenCE systems' (European Commission) <https://cordis.europa.eu/project/id/312651> (in English)

Авдєєва Г. К.
Цифрові докази і системи штучного інтелекту у правозастосовній діяльності

Розглянуто актуальні проблеми використання цифрових доказів у правозастосовній діяльності, надано пропозиції щодо їх розв'язання, розмежовано поняття «електронний доказ» і «цифровий доказ». Аналізом 64 рішень українських судів доведено, що визнання допустимими цифрових доказів спричиняє певні труднощі. Запропоновано доповнити Кримінальний процесуальний кодекс України нормами, які містили б визначення понять «цифрові докази» та «електронні докази», докладний порядок вилучення цифрової інформації, її огляду, фіксації і зберігання, алгоритм оцінки достовірності цифрового доказу за певними критеріями. Поліпшити ефективність використання цифрових доказів у судочинстві рекомендовано шляхом розробки настанов для слідчих, суддів, прокурорів і співробітників оперативно-розшукових органів щодо роботи із ними.

Досліджено роль технологій штучного інтелекту у правоохоронній діяльності, вивчено можливості їх використання в умовах війни, визначено форму та зміст правового регулювання процесів використання систем штучного інтелекту у правозастосовній діяльності, сформульовано принципи та випадки обмеження їх використання. Пропонується формувати законодавство України щодо штучного інтелекту на основі таких основних принципів: повага до основних прав і свобод людини, запобігання будь-якій дискримінації, висока якість та безпека при обробці даних та процесуальних рішень, прозорість, неупередженість, справедливість. Також слід

ураховувати, що процедура доказування у процесуальній діяльності відрізняється від автоматичного аналізу даних системою штучного інтелекту, який може враховувати недостовірні або підроблені дані, неправдиві показання свідка або потерпілого, помилкові висновки експерта та ін. Через це системи штучного інтелекту можуть слугувати лише допоміжним інструментом уповноважених осіб під час прийняття ними процесуальних рішень. Повністю автоматизувати ці процеси в Україні поки що зарано.

Ключові слова: *цифрові докази, електронні докази, допустимість доказів, штучний інтелект, правозастосовна діяльність.*

Avdeeva G. K.

Digital evidence and artificial intelligence systems in legal activity

Current problems of using digital evidence in legal activities are considered, suggestions for their solution were given, the concepts of «electronic evidence» and «digital evidence» are differentiated. An analysis of 64 decisions of Ukrainian courts showed that recognizing digital evidence as admissible entails certain difficulties. It is suggested to supplement the Criminal Procedure Code of Ukraine with rules containing a definition of the concepts «digital evidence» and «electronic evidence», a detailed procedure for examining digital information, its recording and storage, an algorithm for assessing the reliability of digital evidence according to certain criteria. It is recommended to improve the effectiveness of applying digital evidence in legal proceedings by developing recommendations for investigators, judges, prosecutors and employees of operational investigative agencies regarding how to work with them.

The role of artificial intelligence technologies in law enforcement activities and the possibilities of their use in war conditions have been studied, the form and content of legal regulation of the processes of using artificial intelligence systems in law enforcement activities have been determined, and the principles and limitations of their use have been formulated. It is suggested to formulate Ukrainian legislation regarding artificial intelligence on the basis of the following basic principles: respect for fundamental human rights and freedoms, prevention of any discrimination, high quality and safety when processing data and making procedural decisions, transparency, impartiality, fairness. It should also be taken into account that the procedure of proof in procedural activities differs from the automatic analysis of data by an artificial intelligence system, which can consider unreliable or fake data, false testimony, erroneous expert conclusions, etc. Therefore, artificial intelligence systems can only serve as an auxiliary tool for authorized persons when making procedural decisions. It is too early to fully automate these processes in Ukraine.

Key words: *digital evidence, electronic evidence, admissibility of evidence, artificial intelligence, legal activity.*

Стаття надійшла до редакції:22.10.2023 р.
Прийнята до друку: 20.11.2023 р.