УДК 347.94:004
DOI https://doi.org/10.32782/2524-0374/2020-8/20

НАСТАНОВИ РАДИ ЄВРОПИ ЩОДО ЕЛЕКТРОННИХ ДОКАЗІВ: ШЛЯХИ УДОСКОНАЛЕННЯ

THE COUNCIL OF EUROPE GUIDELINES ON ELECTRONIC EVIDENCE: WAYS TO IMPROVE

Каламайко А.Ю., к.ю.н.,
асистент кафедри цивільного процесу
Національний юридичний університет імені Ярослава Мудрого

Нещодавно Рада Європи прийняла перші Настанови щодо електронних доказів у цивільному та адміністративному судочинстві, однак вони вже вимагають певних змін та доповнень, щоб відповідати реаліям правозастосовної діяльності. Вбачається, що доповнені Настанови мають надавати більше практичних порад судам та юристам, що стосуються електронних доказів, а також інших аспектів інформаційно-комунікаційних технологій, які все ширше впроваджуються в судочинство. Було визначено декілька аспектів щодо використання судами Настанов, зокрема щодо швидкого розвитку систем онлайн-вирішення спорів та використання алгоритмів штучного інтелекту в судових системах. Основна увага в цій роботі зосереджена на можливих удосконаленнях, які можуть знадобитися, а також на елементах, що були вилучені на завершальному етапі підготовки Настанов. Існує думка, що деякі пункти та визначення слід відновити в Настановах, оскільки їх вилучення не було достатньо обґрунтованим. В основному це стосується фундаментального принципу прав людини, оскільки стрімке провадження технологій, яке в перспективі має покращити доступ до правосуддя, може призвести до нерівності сторін у процесі через їхню необізнаність щодо можливостей таких технологій. Електронізація може революціонізувати доступ до правосуддя для учасників судових процесів, наприклад для осіб, яким зараз важко отримати доступ до судів, а також покращити доступність шляхом надання дешевих та ефективних засобів для вирішення суперечок. Крім того, цей процес зачіпає також національні процедури щодо електронних доказів. В інтересах забезпечення права на справедливий судовий розгляд слід регулярно оновлювати Настанови, враховуючи та відображаючи технологічний розвиток, нові бізнес-моделі та еволюцію судової практики, тим самим роз'яснюючи як судам, так і учасникам процесу, як отримати максимум користі від електронних технологій у судовому процесі.

Ключові слова: електронні докази, онлайн-вирішення спорів, штучний інтелект, хмарні обчислення, блокчейн.

The Council of Europe has recently adopted the first Guidelines on Electronic Evidence in Civil and Administrative Proceedings (the Guidelines), but they already require some changes and additions to reflect the realities of law enforcement. It is seen that the amended Guidelines should provide more practical advice to courts and lawyers on electronic evidence, as well as other aspects of information and communication technologies that are increasingly being introduced in the judiciary. Several aspects of the use of the Guidelines by courts have been identified, in particular the rapid development of online dispute resolution systems and the use of artificial intelligence algorithms in judicial systems. The focus of this paper is on possible improvements that may be needed, as well as on elements that were removed at the final stage of preparation of the Guidelines. There is an opinion that some points and definitions should be restored to the Guidelines, as their removal was not sufficiently justified. This mainly concerns the fundamental principle of human rights, as the rapid implementation of technology, which in the long run should improve access to justice, can lead to inequality in the process due to their ignorance of the possibilities of such technology. Digitalization can revolutionize access to justice for litigants, such as those who currently find it difficult to access courts, and improve accessibility by providing cheap and effective means of resolving disputes. In addition, this process also affects national procedures for electronic evidence. In the interests of ensuring the right to a fair trial, the Guidelines should be regularly updated, taking into account and reflecting technological developments, new business models and the evolution of case law, thus explaining to both courts and litigants how to make the most of electronic technologies in court process.

Key words: electronic evidence, online dispute resolution, Artificial Intelligence, cloud computing, blockchain.

Вступ. Рада Європи прийняла Настанови щодо електронних доказів у цивільному та адміністративному праві (далі – Настанови) лише нещодавно, 30 січня 2019 року [1]. Обов'язковим документом до Настанов є Пояснювальний меморандум, який пояснює положення Настанов та розкриває джерела, які були використані в Настановах. Метою даної статті є визначити, чи вже є необхідним перегляд Настанов. Це особливо важливо, оскільки Настанови потрібно час від часу оновлювати і для цього слід використовувати перший досвід їх застосування. Принагідно зауважити, що Рада Європи працює над керівництвом щодо врегулювання онлайн-суперечок (далі – ODR), яке також впливає на електронні докази. Вже в 2016 році було проведено дослідження щодо можливості Європейського комітету з питань правового співробітництва (далі – CDCJ) Ради Європи здійснити діяльність щодо механізмів онлайн-врегулювання суперечок з посиланням на статті 6 та 13 Європейської конвенції з прав людини (далі – ЄКПЛ). На продовження цього техніко-економічного обґрунтування CDCJ вирішив розпочати в 2017 році роботу з підготовки технічного дослідження як першого кроку діяльності. Це технічне дослідження було завершено та представлено CDCJ на його 93-му пленарному засіданні (14–16 листопада 2018 р.), яке затвердило його публікацію на своєму веб-сайті. Діяльність продовжується з підготовкою до кінця 2020 року проектів керівних принципів, спрямованих на забезпечення сумісності механізмів ODR зі статтями 6 та 13 ЄКПЛ.

Крім того, зростаюча потреба у використанні електронних доказів у цивільних та адміністративних провадженнях свідчить про розвиток регулювання законодавства Європейського Союзу. Положення про електронну ідентифікацію та послуги довіри для електронних транзакцій на внутрішньому ринку (далі – Регламент eIDAS) зазначає різні аспекти використання електронних доказів (такі як послуги довіри, електронні печатки, електронна відмітка часу, електронна зареєстрована служба доставки, електронний підпис) [2]. Крім того, Регламент eIDAS визначає основний принцип, згідно з яким електронні докази не повинні позбавлятись юридичної сили та допустимості як доказу в судовому процесі лише на тій підставі, що воно знаходиться в електронній формі (Стаття 25 (1), 35 (1), 41 (1), 43 (1) Регламенту eIDAS).

У свою чергу Пропозиція про внесення змін до Регламенту (ЄС) No 1206/2001 від 28 травня 2001 року про співпрацю між судами держав-членів у збиранні Європейською Комісією доказів у цивільних або комерційних справах встановлює, що сучасні комунікаційні технології [3], зокрема відеоконференції, які є важливим засобом для спрощення та прискорення збору доказів, наразі використовуються не в повному обсязі. Отже, пропозиція визнає, що прямий збір доказів за допомогою відеоконференції

повинен бути одним із засобів доказування. Слід забезпечити рівний режим та доказову цінність електронних доказів [4].

Автор не має наміру просто переказувати або узагальнювати існуючі Настанови або прийняту ними процедуру. Читачам цієї статті пропонується ознайомитись як з Настановами [1], так і з пояснювальною запискою [5]. Основна увага в цій роботі зосереджена на можливих удосконаленнях, які можуть знадобитися. Посилання на оригінальну версію Настанов робляться лише за потреби. Також буде доречним прокоментувати розділи, вилучені на завершальному етапі підготовки. Існує думка, що деякі пункти та визначення слід відновити до Керівних принципів, оскільки їх вилучення не було достатньо обґрунтованим. В основному це стосується фундаментального принципу прав людини. Окрім того, Настанови повинні безпосередньо посилатися на використання блокчейну та хмарних обчислень для захисту або обробки електронних доказів.

Окрім загального питання про можливий перегляд, існує низка додаткових конкретних академічних питань, на які потрібно відповісти. Чи повинні переглянуті Настанови надавати більше практичних порад судам та юристам стосовно електронних доказів? Чи повинні такі Настанови бути спрямовані на гармонізацію національного законодавства держав-членів чи продовжувати встановлюватися на рівні загальних принципів, що враховують усі різні правові системи? Чи слід використовувати нові правила ЄС щодо електронних доказів та постійної роботи на Гаазькій конференції як джерело натхнення для розроблення переглянутих керівних принципів?

Нові правозастосовні проблеми, які потребують внесення змін до Настанов

Суди та адміністративні органи щодня розглядають справи, що стосуються електронних доказів, поданих сторонами та іншими особами, які беруть участь у цивільному чи адміністративному провадженні [6, с. 4]. За останні роки цей процес пришвидшився. Це також безпосередньо пов'язано з розробкою систем онлайн-вирішення спорів (Online Dispute Resolution, ODR), частіше паралельно із запровадженням алгоритмів штучного інтелекту (тобто аналізу даних) у судові системи. Наразі можна говорити про те, що в зарубіжній літературі склалося два підходи до розуміння поняття ODR – вузький та широкий. Вузький підхід до розуміння зазначеного поняття охоплює собою лише онлайн ADR. Натомість широкий підхід охоплює весь спектр розгляду спорів онлайн: як онлайн ADR, так і онлайн-суди [7, с. 67]. Наприклад, у Польщі процедура отримання платіжних доручень повністю електронна. Претензія подається через індивідуальний рахунок, відкритий на спеціальній ІТ-платформі. Всі акти та документи доступні в Інтернеті. У Литві відеоконференції можуть бути використані в цивільних процедурах, оскільки кожен суд обладнаний принаймні одним залом для відеоконференцій, а кожен зал має аудіообладнання.

Обидва ці фактори значно посилюють оцифрування процедур та їх важливість [8]. Це також може революціонізувати доступ до правосуддя для учасників судових процесів, наприклад для осіб, яким зараз важко отримати доступ до судів [9]. Цифровізація також покращує доступ до суду шляхом надання дешевих засобів для вирішення суперечок [10]. Цей процес зачіпає також національні процедури щодо електронних доказів.

Новим викликом, який не відображений у Настановах, є швидка поява штучного інтелекту (Artifical Intelligence, AI). AI – це широка область інформаційно-комунікаційних технологій, що дозволяє автоматизувати міркування [11]. Це дозволяє приймати автоматизовані рішення, робить рекомендації та прогнози ефективними та доступними [12]. На практиці це означає, що багато цивільних та адміністративних проваджень, заснованих на трудомісткій судовій роботі, можна автоматизувати [13, с. 539–574]. Він може базуватися на повторенні зразків фактичних сценаріїв та юридичній категоризації спорів [14, с. 211–240]. Натепер компоненти AI впроваджуються в судових системах, особливо щодо аналізу даних [15]. Це також означає, що норми щодо електронних доказів повинні бути впорядковані, щоб забезпечити можливість впровадження AI у процесі. Наприклад, AI не може обробляти дані, представлені сторонами в письмовій формі (роздруківки – у цьому відношенні див. Вказівку № 9 у Настановах).

Електронні докази багато в чому відрізняються від інших видів доказів [16; 17; 18; 19; 20]. Електронними доказами (також їх називають цифровими доказами) можуть бути тексти, відео, фотографії або звукозаписи [21]. Дані можуть надходити з різних джерел, таких як мобільні телефони, веб-сайти, комп'ютери або реєстратори GPS [22, с. 14–17]. Сюди також належать дані, що зберігаються на відстані в хмарних обчисленнях, або все більше використання систем AI. Типовим прикладом електронних доказів є електронні дані, отримані з електронного пристрою, що містить відповідні метадані [22, с. 10]. З цією проблемою пов'язані технології, які сьогодні частіше використовуються для забезпечення доказів, такі як розподілені регістри (*блокчейн*) [23; 24]. Blockchain – це відносно нова технологія, яка може забезпечити більшу впевненість та безпеку електронних доказів [25; 26; 27]. Його можна визначити як розподілений регістр, який містить перелік записів (блоків), підключених та захищених криптографією та зареєстрованих у децентралізованій еквівалентній мережі. Це робить технологію блокчейну дуже корисною для доказових цілей. Однак прямого посилання на блокчейн у Настановах немає. Лише в Пояснювальному меморандумі ця технологія згадується як така, що є стійкою до модифікації даних. Це одне з головних нових питань, яке слід додатково розглянути в переглянутих Настановах.

Окрім Настанов, до цього часу було прийнято лише декілька юридичних документів, що сприяють обробці електронних доказів у цивільних та адміністративних провадженнях на міжнародному, європейському та національному рівнях. Існують лише деякі загальні та вже застарілі положення, такі як: Типовий закон про електронну комерцію, прийнятий Комісією 12 червня 1996 року після її 605-го засідання та Генеральною Асамблеєю в Резолюції 51/162 на її 85-му пленарному засіданні 16 Грудня 1996 р., включаючи додаткову статтю 5-біс, прийняту Комісією на її 31-му засіданні в червні 1998 р. Типовий закон про електронні підписи був прийнятий Комісією на її 727-му засіданні 5 липня 2001 р. Також керівні принципи, прийняті за межами Європи, тобто Проект типового закону Співдружності про електронні докази, Типові керівні принципи політики та законодавчі тексти (Гармонізація політики ІКТ, законодавство та регулятивні процедури в Карибському басейні, Міжнародне бюро розвитку телекомунікацій Союзу телекомунікацій, Женева, 2013).

Як у законодавстві, так і в судовій практиці все ще існує розрив щодо ключових технологічних принципів роботи з електронними доказами, зокрема, коли ми говоримо про використання хмарних обчислень, блокчейну або алгоритмів AI для забезпечення, подання та аналізу електронних доказів. Тому необхідність перегляду Настанов невпинно зростає. Вони повинні бути адаптовані до сучасного етапу розвитку цифровізації судів. Через такі причини ми вважаємо, що перший перегляд повинен супроводжуватися прийняттям як керівних принципів, так і визначень таких нових технологій, як хмарні обчислення, алгоритми блокчейну або AI.

На нашу думку, докази, отримані за допомогою алгоритму, хмарних обчислень, блокчейну або іншим способом, в електронному вигляді можуть бути досить надійними та достовірними в цивільних та адміністративних

процесах. На практиці найважливіше, як можна збирати такі типи доказів та які вимоги щодо прийнятності повинні бути встановлені. Вони можуть бути зібрані за допомогою спеціальних програм, а це означає, що може знадобитися певний досвід. Однак кожен із цих конкретних доказів має свою особливість. Наприклад, блокчейн є надзвичайно стійким до модифікації даних. Після запису дані в будь-якому даному блоці не можуть бути змінені в зворотному порядку без зміни всіх наступних блоків, що вимагає змови більшості мережі. Це робить блокчейн придатним для доказових цілей. Однією з можливостей забезпечити законність цифрового запису, зареєстрованого електронним способом у блокчейні, може бути декларація кваліфікованої особи. Подібним чином автентифікація доказів за допомогою хмарних обчислень та алгоритму може бути корисною та першим кроком у процесі аутентифікації. Однак якщо аутентифікація недостатня, експертиза може бути особливо актуальною.

Запропоновані доповнення до Настанов

Вбачається, що низка нових проблем має бути вирішена вдосконаленням та доповненням Настанов. Передусім ключовий принцип щодо прав людини слід відновити серед основних принципів Настанов. Його вилучення на завершальній стадії підготовки Настанов звучить дивно, оскільки Керівні принципи були підготовлені Радою Європи відповідно до практики Європейського суду з прав людини.

Можна стверджувати, що, очевидно, Настанови слід читати разом з іншими керівними принципами та практикою ЄСПЛ. Тим не менше, Настанови регламентують особливо чіткий тип доказів, на які застосування загальних правил захисту прав людини та практики ЄСПЛ може вимагати певного погляду. Більше того, явне посилання на права людини (наприклад, право на приватне життя) може привернути увагу практикуючих юристів та вимагати врахування захисту прав людини під час роботи з електронними доказами в кожному конкретному випадку.

На нашу думку, Настанови повинні складатися таким чином, щоб посилити ефективність та якість правосуддя. Це особливо важливо, оскільки норми щодо електронних доказів, прийняті натепер у державах-членах, не в достатній мірі зосереджені на процесуальних гарантіях, а на тому, щоб суперечка була ефективно вирішена економічно [28]. Це виклик забезпечити, щоб правила електронних доказів відповідали праву на справедливий судовий розгляд, яке встановлено у статті 6 Європейської конвенції з прав людини. Дуже важливо, щоб Настанови сприяли більш ефективному доступу до правосуддя. Переоблена версія Настанов повинна бути складена таким чином, щоб питання цифрового розриву було адекватно вирішене. Важливо встановити, що сторони в процесі не потрапляють у невигідне становище через їх недостатнє розуміння того, як використовуються технології. Процесуальні норми щодо електронних доказів повинні бути максимально зручними для користувача в тому значенні, що вони не працюють таким чином, що може зашкодити інтересам будь-якої зі сторін.

Як зазначалося вище, основний принцип Настанов, який був видалений на завершальній стадії підготовки, посилався на верховенство права та неприпустимість електронних доказів, отриманих незаконним способом (наприклад, унаслідок порушення конфіденційності або даних правила нерозглошення). Прикладом може бути вилучення електронного пристрою без рішення суду, передбаченого законом, а також докази, отримані стороною шляхом злому ІТ-системи. Наприклад, із практики ЄСПЛ випливає, що докази, зібрані внаслідок порушення роботодавцем принципів захисту приватності працівника, можуть бути неприпустимими через порушення принципу пропорційності. У фундаментальній справі *Bărbulescu v. Romania* Велика палата ЄСПЛ встановила, що румунські суди, переглядаючи рішення роботодавця про звільнення працівника після моніторингу його електронних комунікацій, не змогли встановити справедливий баланс між правом працівника поважати своє приватне життя та листування і правом свого роботодавця вживати заходів для забезпечення безперебійного функціонування компанії [29]. Докази, зібрані таким чином (з порушенням права на приватне життя), не сумісні з правом на справедливий суд і не повинні бути прийнятними. Тим не менше, виникає складне питання, коли електронні докази збираються без відома та прийняття особи, але це свідчить про те, що особа вчинила злочин. У нещодавній справі *López Ribalda and others v. Spain* Велика палата ЄСПЛ установила, що спостереження за працівниками прихованими камерами (про що працівники не знали) відповідає праву на приватне життя, оскільки відеозаписи використовувались лише для того, щоб відстежувати винних у збитках товарів із магазину та вживати проти них дисциплінарні заходи [30]. Також суд установив, що національні норми забезпечували суттєві процесуальні гарантії в цій справі. Отже, переглянута версія Настанов повинна включати цей значний розвиток у збір електронних доказів.

Інший розділ, що вимагає більш детального розроблення в Настановах, полягає в тому, як можна оскаржити автентичність або цілісність електронних доказів (порівняйте існуючі вказівки № 18–24 Настанов), зокрема щодо доказів, отриманих із хмарних обчислень, блокчейну або за допомогою алгоритмів AI. Настанови можуть передбачати відповідні конкретні механізми, наприклад, у формі додатку до Настанови, що пояснює характеристики блокчейну, з метою полегшення такого виклику. Більше того, в Настановах повинно бути чітко визначено, що сторонам слід повністю дозволити оскаржувати висновки експертів, якщо такі докази, ймовірно, визначатимуть результат розгляду справи (порівняйте вихідну настанову № 18 Настанов). У зв'язку з цим принципи правової визначеності та захисту законних сподівань сторін вказують на те, що сторони можуть покладатися на попередні рішення, прийняті судом, коли факти справи, що розглядається, були подібними до тих, що були в поточному провадженні. Рекомендується, щоб сторони могли структурувати свої докази на основі таких рішень. Отже, з міркувань юридичної визначеності та послідовності переглянута версія Настанов повинна враховувати такі рішення щодо переваги, відступаючи від них лише там, де для цього є вагомі та достатні причини. Варто зазначити, що ЄСПЛ визнав, що принцип правової визначеності передбачає, що сторона, яка покладається на оцінку, зроблену судом у попередній справі щодо питання, котре також виникає в цій справі, може законно розраховувати на виконання судом попереднього рішення, якщо тільки існує поважна причина відступу від нього (Siegle v. Romania, §§ 38–39, Rozalia Avram v. Romania, §§ 42–43 §§ 38–39).

Нові способи ідентифікації джерела доказів, тобто у випадку доказів, отриманих із блокчейну, використання алгоритмів AI або хмарних обчислень, також повинні бути представлені в Настановах. Відсутні пункти в існуючій версії Настанов – це саме ідентифікація джерела доказів у випадку блокчейну, хмарних обчислень або алгоритмів AI. Важливо, щоб не було питання про шахрайські дані. Відокремлення цифрової ідентичності від фізичної породжує проблеми, пов'язані з джерелом доказів. У зв'язку з цим Настанови можуть містити чіткі вказівки щодо того, що підтвердження особи оператором платіжної системи може використовуватися як механізм ідентифікації.

Ще більше уваги в переглянутій версії Настанов слід приділити усвідомленню потенційного доказового значення метаданих [31, с. 28]. Метадані в даний час визначаються в Настановах як дані, що стосуються інших даних. Мальовнича метафора – називати це «цифровим відбитком» електронних доказів. Він може містити важливі

доказові дані, такі як дата та час створення або модифікації файлу чи документа, дані про автора чи дату та час відправлення. Через технологічні труднощі переглянута версія Настанов повинна наводити приклади того, як метадані слід збирати та оцінювати на практиці. Оскільки для збору метаданих можуть знадобитися певні додаткові комп'ютерні програми та конкретні знання, Настанови можуть указувати, як учасники процесу повинні вирішувати це практичне завдання. Крім того, оскільки метаданими можуть маніпулювати, Настанови можуть пояснити, як суди повинні оцінювати метадані та виявляти, чи вони були змінені.

Настанови також повинні охоплювати проблему маніпуляцій з електронними доказами та шляхи виявлення фальсифікації доказів (порівняйте існуючі вказівки № 10–11 Настанов). На наш погляд, тягар установлення достовірності електронних доказів, що здійснюється стороною, яка прагне покластись на неї (наприклад, шляхом надання заяви експерта), повинен регулюватися в переглянутих Настановах. Судді та юристи також повинні пройти обов'язкову підготовку (а не просто бути проінформованими) про розвиток інформаційних технологій та процесів, які можуть вплинути на цінність електронних доказів.

Однією з найскладніших частин, яку потрібно врегулювати, є визначення законодавства, яке застосовується до доказів, отриманих стосовно транскордонних справ, та доступних засобів правового захисту, наприклад у випадку невиконання судових повноважень та цілісності судового розгляду (неповага до суду) або завідомо неправдивих показань. Існуючі Настанови № 12–13 не є задовільними в цьому відношенні, хоча ми розуміємо, що це питання дуже складне і вимагає великої додаткової роботи. Однак ми вважаємо, що це саме правильний виклик для переглянутих настанов щодо забезпечення стандартів передачі електронних доказів між іноземними судами [32]. Корисно, що Європейський Союз працює паралельно над такими новими стандартами. Тим не менше, завдання Ради Європи полягає не в тому, щоб повторити чи поширити рішення Європейського Союзу на інші держави, а навпаки, розробити більш універсальні правила. Слід взяти до уваги, що хоча використання доказів може бути суто національним, частіше воно є транскордонним. Прикладом може бути розташування в іноземній країні хмарних обчислень або інфраструктури блокчейнів, що використовуються для обробки або зберігання даних, або місцезнаходження постачальника, який дозволяє зберігати або обробляти дані. У переглянутій версії Настанов слід зробити акцент на безпосередній співпраці між судами та постачальниками хмарних послуг у транскордонних справах та надати конкретні вказівки, якими повинні бути результати такої співпраці (наприклад, щодо забезпечення вилучення електронних доказів) [33, с. 671–682].

Хмарні обчислення – прекрасний приклад транскордонних технологій за своєю природою. Спільний доступ до даних у хмарі означає зберігання різних частин бази даних на різних серверах, які можуть бути розташовані в різних фізичних місцях [34, с. 3–4]. Зберігання даних, які можуть становити електронні докази в хмарі, вже стало звичною практикою. Глобальний характер Інтернету та зростаюче використання хмарних послуг спростовують припущення, що доступ до даних та їх обробка є суто національними. Проблема полягає в тому, що між національними процесуальними нормами щодо вивезення доказів за кордон існують суттєві відмінності. Суди, які використовують докази за кордоном, повинні враховувати ці відмінності.

Вищевикладене не має на меті представити вичерпний перелік питань, що виникають у контексті електронних доказів і які можуть стати предметом переглянутих Настанов. Вони повинні враховувати та відображати всі відповідні та останні технологічні розробки, нові бізнес-моделі та еволюційну прецедентну практику.

На нашу думку, переглянута версія Настанов не повинна встановлювати обов'язкові правові стандарти. За своєю суттю вона не є зобов'язуючим документом (т.з. *м'яке право*) і не має на меті гармонізувати національне законодавство держав-членів. Також Настанови не слід тлумачити як такі, що передбачають певну юридичну цінність електронних доказів. Нарешті, Настанови повинні бути сформульовані таким чином, щоб ураховувати різні правові системи держав-членів Ради Європи. Тим не менше, рекомендується, щоб вони мали характер практичного набору інструментів. Настанови повинні бути не лише декларацією принципів, а і практичними вказівками. З цієї причини ми вважаємо, що Настанови можуть бути доповнені більш технічними та детально розробленими додатками. Прикладом може бути перелік проблем, пов'язаних із використанням хмарних обчислень для забезпечення та вилучення електронних доказів [35].

Висновки. Настанови, прийняті Радою Європи, є першим міжнародним документом, який пояснює, як суди повинні обробляти електронні докази в цивільних та адміністративних процесах. Їх було прийнято відповідно до національного законодавства держав-членів Ради Європи та стандартів прав людини, встановлених у судовій практиці ЄСПЛ. Тим не менше, на нашу думку, через швидкі зміни в технології та правовому регулюванні електронних доказів Настанови слід переглянути. Крім того, поточна версія Настанов не стосується деяких особливо важливих аспектів електронних доказів.

Електронні докази, пов'язані з хмарними обчисленнями, блокчейном, алгоритмами AI, навряд чи пояснюються в Настановах або Пояснювальному меморандумі. Однак такі типи електронних доказів є особливо складними для судів та юристів, тому що стосуються оцифровки суду, і бракує міжнародних стандартів, які регулюють ці питання. У переглянутій версії Настанов слід не лише визначити такі типи електронних доказів, але й пояснити особливості, як їх слід збирати та оцінювати на практиці.

Також пропонується додавати нові розділи до Настанов. Поточна версія Настанов та національне регулювання держав-членів зосереджені не в достатній мірі на процедурних гарантіях, а на тому, щоб суперечка була ефективно вирішена економічно. Тим не менше, розвиток судової практики ЄСПЛ щодо збору електронних доказів (за допомогою відеоспостереження) та захисту права на приватне життя є особливо важливим. Збір електронних доказів тісно пов'язаний з правом на приватне життя. Настанови повинні розглядати необхідність захисту права на приватне життя з правом збору електронних доказів та способу встановлення справедливого балансу між цими двома правами.

Іншою важливою сферою, яку слід дослідити в переглянутій версії Настанов, є транскордонна передача електронних доказів. Часто електронні докази можуть знаходитися в іншій країні, ніж суд, який розглядає справу. У такому випадку виникає необхідність передавати інформацію або збирати її у співпраці з іноземним судом (іншими установами та навіть приватними структурами). Існуюча версія Настанов не є задовільною вцьому відношенні, хоча ми розуміємо, що це питання є дуже складним і вимагає широкого розгляду. Однак це якраз правильний виклик для переглянутої версії Настанов забезпечити стандарти передачі електронних доказів як між іноземними судами.

ЛІТЕРАТУРА

1. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies), 30 January 2019, CM(2018)169-add1final. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c
2. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC OJ L 257, 2014.
3. Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (COM/2018/378 final).
4. Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (SWD/2018/285 final).
5. The Explanatory Memorandum to the Guidelines. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0e
6. Biasiotti M., Bonnici J., Cannataci F. Turchi, Introduction: Opportunities and Challenges for Electronic Evidence, in: Handling and Exchanging Electronic Evidence Across Europe / M. Biasiotti et al ; ed. M. Biasiotti. Cham, 2018. P. 4.
7. Цувіна Т.А. Онлайн суди та онлайн вирішення спорів у контексті міжнародного стандарту доступності правосуддя: міжнародний досвід. *Проблеми законності*. 2020. Вип. 149. С. 62–79. URL: http://nbuv.gov.ua/UJRN/Pz_2020_149_7
8. Online Dispute Resolution and Compliance with the Right to a Fair Trial and the Right to an Effective Remedy (Article 6 and 13 of the European Convention of Human Rights). Technical Study on Online Dispute Resolution Mechanisms – prepared by Prof Julia Hörnle, CCLS, Queen Mary University of London, Matthew Hewitson (South Africa) and Illia Chernohorenko (Ukraine), Strasbourg, 1 August 2018, CDCJ(2018)5.
9. Hörnle J. Cross-border Internet Dispute Resolution. Cambridge University Press, 2009.
10. Hörnle J. Encouraging Online Alternative Dispute Resolution (ADR) in the EU and Beyond, European Law Review. 2013. Volume 38 (2). P. 187–208.
11. Recommendation of the OECD Council on Artificial Intelligence, OECD/LEGAL/0449, Adopted on: 22/05/2019. URL: https://legalin- struments.oecd.org/en/instruments/OECD-LEGAL-0449
12. A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Prepared by the Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT). Rapporteur: Karen Yeung, DGI(2019)05.
13. Scherer M. Artificial Intelligence and Legal Decision-Making: The Wide Open? *Journal of International Arbitration*. 2019. Vol. 36. № 5. P. 539–574.
14. ODR: an Artificial Intelligence Perspective, Artificial Intelligence Review / D. Carneiro et al. 2014. Volume 41. P. 211–240.
15. A Definition of AI: Main Capabilities and Scientific Disciplines. Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI Brussels, 18 December 2018. URL: https://ec.europa.eu/digital-single-market/en/news/ definition-artificial-intelligence-main-capabilities-and-scientific-disciplines, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
16. George L. Paul, Foundations of Digital Evidence (American Bar Association), 2008.
17. Paul R. Rice, Electronic Evidence – Law and Practice. 2nd edn. American Bar Association, 2009.
18. Stanfield A. Computer Forensics, Electronic Discovery & Electronic Evidence (LexisNexis Butterworths, 2009), Stephen Mason, ed, Electronic Evidence. 3rd edn, LexisNexis Butterworths, 2017.
19. Mason S. ed, International Electronic Evidence. British Institute of International and Comparative Law, 2008.
20. Каламайко А.Ю. Електронні докази в цивільному процесі : монографія. Харків : Право, 2017. 176 с.
21. Bonnici J., Tudorica M., Cannataci J. The European Legal Framework on Electronic Evidence: Complex and in Need of Reform, in: Handling and Exchanging Electronic Evidence Across Europe ; ed. M. Biasiotti et al. Cham, 2018. P. 190.
22. Weir G., Mason S. The sources of electronic evidence, in: Electronic Evidence ; ed. S. Mason, D. Seng. London, 2017. P. 14–17.
23. Pilkington M. Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations. Edward Elgar, 2016. URL: https://ssrn.com/abstract=2662660
24. Distributed Ledger Technology: beyond block chain, A report by the UK Government Chief Scientifc Adviser, Government Office for Science. London, 2016. URL: https://www.gov.uk/govern- ment/uploads/system/uploads/attachment_data/ file/492972/gs-16-1-distributed-ledger-technology.pdf
25. Neisse R., Steri G., Fovino I. A blockchain-based approach for data accountability and provenance cracking, w: Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–01 September 2017. P. 14:1– 14:10. URL: https://doi.org/10.1145/3098954.3098958
26. Vukolic M. Rethinking permissioned blockchains, w: ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC 2017), April 2017. URL: http://vukolic. com/rethinking-permissioned-blockchains-BCC2017.pdf
27. Jokubauskas R., Świerczyński M. 'Is revision of the council of Europe guidelines on electronic evidence already needed?' (2020) 16(1) Utrecht Law Review. P. 13–20.
28. Vitkauskas D., Dikov G. Protecting the right to a fair trial under the European Convention on Human Rights: A handbook for legal practitioners, Council of Europe 2017. URL: https://rm.coe.int/protecting-the-right-to-a-fair-trial-under-the-european- convention-on-/168075a4dd
29. ECtHR judgment of 5 September of 2017 in case Bărbulescu v. Romania, petition No. 61496/08.
30. ECtHR judgment of 17 October 2019 in case López Ribalda and others v. Spain, petitions No. 1874/13 8567/13.
31. Schafer B., Mason S. The Characteristics of Electronic Evidence, in: Electronic Evidence: Disclosure, Discovery and Admissibility ; ed. S. Mason, P. Argy, & D. Begg. Butterworth, 2010. P. 28.
32. Svantesson D. Law enforcement cross-border access to data, Preliminary Report, November, 2016.
33. Jerker D., Svantesson D., van Zwieten L. Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution. *Computer Law Security Review*. 2016. Vol. 32. P. 671–682.
34. Vincent M., Hart N. Legal issues in the cloud. *Computers & Law.* 2011. Vol. 79. P. 3–4.
35. "Unleashing the Potential of Cloud Computing in Europe" Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 27.9.2012 COM(2012) 529 final, SWD(2012) 271 final.