

## ПІДХОДИ ДО ВИЗНАЧЕННЯ ТА ВИКОРИСТАННЯ ЦИФРОВИХ ДОКАЗІВ: МІЖНАРОДНИЙ ДОСВІД

### APPROACHES TO THE DEFINITION AND USE OF DIGITAL EVIDENCE: INTERNATIONAL EXPERIENCE

Фортуна Т.Ю., здобувач кафедри конституційного та адміністративного права  
Запорізький національний університет

У статті досліджено міжнародні підходи до визначення та використання цифрових доказів. Вказано, що цифрові докази у міжнародній правозастосовній практиці розглядаються як електронні дані, що відображають дії, події або обставини, значущі для судового розгляду. До них належать журнали дій, електронна пошта, метадані, аудіо- та відеозаписи, скріншоти та інші матеріали, створені чи збережені за допомогою інформаційно-комунікаційних технологій. Міжнародні стандарти визначають основні вимоги до цифрових доказів: цілісність, автентичність та можливість ідентифікації джерела. Для цього використовуються цифрові підписи, хешування та криптографічні методи, що гарантують недоторканність даних. У США, наприклад, Федеральні правила доказів допускають електронні дані лише за умови підтвердження їх достовірності та автентичності. Цифрові докази застосовуються в кримінальному, цивільному та адміністративному процесі, при цьому оцінка здійснюється комплексно з іншими доказами. Судові процедури передбачають технічне відтворення аудіо- та відеоматеріалів, а також залучення експертів для підтвердження достовірності даних.

Зроблено висновок, що на сучасному етапі розвитку людства, де цифрові технології пронизують усі сфери суспільного життя, питання використання цифрових доказів набуває особливої ваги. Адміністративно-правові відносини вже давно не обмежуються лише традиційними формами контролю та регулювання, а дедалі більше переходять у цифровий вимір. Це означає, що у справах про адміністративні правопорушення роль доказів, отриманих і зафіксованих за допомогою технічних засобів, стає визначальною. Міжнародні підходи до визначення та застосування таких доказів відображають різні рівні зрілості правових систем, різні традиції правозастосування та різні пріоритети між забезпеченням ефективності правосуддя і захистом прав людини. Саме тому дослідження міжнародного досвіду у цій сфері має велике теоретичне та практичне значення.

**Ключові слова:** цифрові докази, міжнародний досвід, електронні дані, міжнародні стандарти.

The article examines international approaches to the definition and use of digital evidence. It is indicated that digital evidence in international law enforcement practice is considered as electronic data reflecting actions, events or circumstances significant for judicial proceedings. These include action logs, e-mail, metadata, audio and video recordings, screenshots and other materials created or stored using information and communication technologies. Digital evidence requirements: integrity, authenticity, and source identification. For this, digital signatures, hashing and cryptographic methods are used to guarantee the inviolability of the data. In the United States, for example, the Federal Evidence Rules only allow electronic data if its authenticity and authenticity are confirmed. Digital evidence is used in criminal, civil and administrative proceedings, while the assessment is carried out in a comprehensive manner with other evidence. Court procedures involve the technical reproduction of audio and video materials, as well as the involvement of experts to confirm the authenticity of the data.

It is concluded that at the present stage of human development, where digital technologies permeate all spheres of public life, the issue of using digital evidence acquires special importance. Administrative and legal relations have long been not limited to traditional forms of control and regulation, but are increasingly moving into the digital dimension. This means that in cases of administrative offenses, the role of evidence obtained and recorded with the help of technical means becomes decisive. International approaches to the definition and application of such evidence reflect different levels of maturity of legal systems, different traditions of law enforcement and different priorities between ensuring the effectiveness of justice and the protection of human rights. That is why the study of international experience in this area is of great theoretical and practical importance.

**Key words:** digital evidence, international experience, electronic data, international standards.

**Постановка проблеми.** Цифрові докази у міжнародній правозастосовній практиці розглядаються як електронні дані, що відображають дії, події або обставини, значущі для судового розгляду. До них належать журнали дій, електронна пошта, метадані, аудіо- та відеозаписи, скріншоти та інші матеріали, створені чи збережені за допомогою інформаційно-комунікаційних технологій.

Міжнародні стандарти визначають основні вимоги до цифрових доказів: цілісність, автентичність та можливість ідентифікації джерела. Для цього використовуються цифрові підписи, хешування та криптографічні методи, що гарантують недоторканність даних. У США, наприклад, Федеральні правила доказів допускають електронні дані лише за умови підтвердження їх достовірності та автентичності.

Цифрові докази застосовуються в кримінальному, цивільному та адміністративному процесі, при цьому оцінка здійснюється комплексно з іншими доказами. Судові процедури передбачають технічне відтворення аудіо- та відеоматеріалів, а також залучення експертів для підтвердження достовірності даних.

**Мета статті** – дослідити міжнародні підходи до визначення та використання цифрових доказів.

**Виклад основного матеріалу.** Міжнародні стандарти та рекомендації, зокрема Будапештська конвенція [1]

та ISO/IEC 27037:2012 [2], встановлюють порядок збору, зберігання, аналізу та передачі цифрових доказів, а також захист від їх пошкодження чи втрати. Європейська комісія рекомендує національним правовим системам розробляти регламенти для забезпечення належного використання цифрових доказів, включно з метаданими та логами комп'ютерних систем.

Разом із тим, міжнародна практика фіксує певні проблеми, як-то різні підходи до допустимості доказів у різних юрисдикціях, технічні складнощі перевірки автентичності та питання захисту персональних даних. Водночас стандартизація процедур та розвиток технологій сприяють підвищенню ефективності використання цифрових доказів у правовому полі.

Варто вказати, що Європейський Союз розробив власну нормативну базу, спрямовану на врегулювання питань, пов'язаних із використанням електронних доказів. Зокрема, було ухвалено Регламент (ЄС) 2023/1543, що регулює порядок застосування Європейських ордерів на отримання та збереження електронних доказів у кримінальних провадженнях, а також у межах виконання покарань, пов'язаних із позбавленням волі після винесення вироку. Даний Регламент встановлює чіткі правила та процесуальні гарантії для національних органів, зобов'язуючи провайдерів послуг, що функціонують

у межах іншої держави-члена, зберігати та надавати електронні дані на запит компетентних установ інших юрисдикцій ЄС [3]. Додатково було ухвалено Директиву (ЄС) 2023/1544, яка забезпечує уніфікацію правил щодо визначення уповноважених установ та призначення офіційних представників із метою збору електронних доказів у кримінальних процесах [4].

Відповідно до п. 8 ст. 3 Регламенту 2023/1543, електронні докази поділяються на три категорії, зокрема дані абонента, дані трафіку та дані змісту. До першої групи належать ідентифікаційні відомості користувача, зокрема ім'я, дата народження, поштова та електронна адреса, банківські реквізити для оплати рахунків, контактні номери та інші реєстраційні дані. Дані трафіку охоплюють інформацію, пов'язану з функціонуванням послуг, а саме маршрут і джерело повідомлень, технічні параметри взаємодій, місцезнаходження пристрою, дату, час, тривалість з'єднання, розмір і формат переданих файлів, а також використані протоколи чи алгоритми стиснення. Третя група – це дані змісту, зокрема включає текстову, графічну, відео-, аудіо- та іншу інформацію, яка зберігається або передається у цифровому форматі.

Окремо варто уваги досвід Китайської Народної Республіки. У 2012 році до Кримінально-процесуального кодексу КНР було включено електронні докази як самостійну категорію доказів, проте закон не містив докладного визначення даного поняття [5]. Подальше роз'яснення було закріплено у спеціальному Положенні «Про вирішення деяких питань щодо збирання, отримання та аналізу електронних даних у кримінальних справах». У цьому акті електронні докази визначаються як інформація, що була зібрана під час кримінального провадження, збережена та передана в електронному вигляді й може бути використана в якості доказової бази.

Документ відносить до електронних доказів веб-сайти, блоги, мікроблоги, сторінки у соціальних мережах, ідентифікатори користувачів у додатках (наприклад, WeChat), форуми, онлайн-сховища, а також різні форми комунікацій (електронна пошта, повідомлення у месенджерах, мобільні повідомлення). Значне місце займають дані, що ідентифікують користувача, отримані при реєстрації, здійсненні електронних транзакцій або у журналах системних реєстрацій. Положення також встановлює процесуальний порядок отримання таких доказів, наголошуючи на необхідності дотримання спеціальних технічних стандартів та залучення щонайменше двох слідчих [6].

Важливу роль у формуванні міжнародних підходів до електронних доказів відіграють міжнародні організації. Так, у 2019 році Інтерпол організував міжнародну зустріч, присвячену проблематиці електронних доказів. У ході дискусій було визначено ключові проблеми, пов'язані з їх використанням, та вироблено рекомендації для правоохоронних і законодавчих органів. Зокрема, при здійсненні обшуку чи виїмки електронних носіїв наголошувалося на необхідності поводитися з ними так само, як і з традиційними матеріальними доказами, із дотриманням принципів їхньої цілісності. Було підкреслено, що деякі цифрові пристрої є надзвичайно чутливими, зокрема вони можуть пошкоджуватися під впливом електромагнітних полів або змінювати свій вміст у процесі транспортування без належного резервного копіювання [7].

Отже, використання електронних доказів у кримінальному судочинстві залишається складним і динамічним напрямом розвитку процесуального права. З одного боку, такі докази створюють нові можливості для ефективної роботи правоохоронних органів, з іншого породжують низку викликів, пов'язаних із конфіденційністю, надійністю та міжнародною координацією. Для України, яка перебуває на шляху євроінтеграції, надзвичайно важливим є узгодження національного законодавства з правом ЄС у сфері кримінального процесу та забезпечення належ-

ного рівня співпраці з державами-членами. Це дозволить не лише підвищити ефективність боротьби з кіберзлочинністю, а й сприятиме становленню України як повноправного учасника європейського правового простору.

У державах романо-германської правової системи будь-які об'єктивні факти, що здатні підтвердити реальний стан справи, можуть бути прийняті судом. Тому навіть у випадках, коли електронні докази не отримали чіткого законодавчого закріплення, вони все ж можуть використовуватися через більш ліберальні підходи до видів доказів. Натомість для англо-американської правової системи, що орієнтована на суворе регулювання доказової бази, найвищу доказову цінність має оригінал документа, а електронні копії часто оцінюються судами неоднозначно.

В різних правових традиціях під електронними доказами розуміють будь-яку інформацію, створену, збережену або передану у цифровій формі, яка може бути залучена для підтвердження або спростування факту, що є предметом судового розгляду [8, с. 11]. Використання електронних доказів в адміністративному судочинстві стає об'єктивною потребою, оскільки суди повинні адаптуватися до сучасних соціально-економічних змін, зумовлених впровадженням електронних послуг. При цьому необхідно враховувати стандарти поведінки з такими доказами та їхню доказову силу, щоб забезпечити їхнє належне застосування та визнання у судовому процесі. Можна припустити, що розвинені країни досягли значного прогресу у впровадженні електронних доказів. Однак на практиці більшість досліджуваних держав досі не мають нормативно визначених правил щодо їхнього використання в адміністративному судочинстві.

Доцільно у контексті нашого дослідження згадати й про Другий Додатковий протокол до Конвенції про кіберзлочинність (Будапештської конвенції) [9], який виступає одним із найважливіших міжнародних правових інструментів, розроблених для посилення механізмів міжнародної взаємодії у сфері протидії кіберзлочинності та забезпечення більш оперативного доступу до цифрових доказів. Документ не лише розширює та уточнює чинні положення Конвенції, але й відповідає на нові виклики, що виникають у зв'язку з розвитком інформаційних технологій і глобальним характером кіберзлочинності. Він передбачає сучасні процедури та стандарти, які дозволяють спростити й прискорити процес збору електронних доказів, а також підвищити результативність розслідувань злочинів, що мають транскордонний характер [10].

Доцільно зазначити, що для України, яка прагне гармонізувати своє законодавство з європейськими стандартами та посилити рівень кіберзахисту, імплементація положень цього Протоколу є не лише зобов'язанням у рамках міжнародних домовленостей, але й стратегічним напрямом розвитку. Вона відкриває нові можливості для розширення співпраці з іноземними партнерами, вдосконалення національної нормативної бази та підвищення ефективності діяльності правоохоронних органів у сфері протидії кіберзлочинності.

Основне завдання Протоколу полягає у доповненні Будапештської конвенції та Першого Додаткового протоколу шляхом створення розширених можливостей для міжнародної співпраці у сфері кібербезпеки [9]. Його положення поширюються на конкретні кримінальні розслідування та судові процеси, що стосуються злочинів, пов'язаних із використанням комп'ютерних систем і даних, а також на збирання електронних доказів у будь-яких категоріях кримінальних справ. Завдяки цьому держави-учасниці отримують інструменти для оперативнішого та більш законного доступу до необхідної інформації [10].

Крім того з метою забезпечення чіткості тлумачення Протокол вводить низку нових визначень. Так, термін «центральный орган» позначає структуру, відповідальну

за координацію взаємної правової допомоги, а «компетентний орган» будь-яку установу, яка має право видавати або виконувати процесуальні заходи, передбачені Протоколом. Особливе значення має визначення «надзвичайна ситуація», що дає підстави для прискореного доступу до даних у випадках, коли існує реальна й невідкладна загроза життю чи безпеці особи. Додатково уточнено поняття «персональні дані» та «сторона, що передає», які є принципово важливими для забезпечення належного рівня захисту приватної інформації [9].

Держави-учасниці Протоколу беруть на себе зобов'язання забезпечувати максимально можливу взаємодію, при цьому дотримуючись принципів поваги до національного суверенітету, прав людини та фундаментальних свобод. Співпраця має здійснюватися в межах внутрішнього законодавства кожної країни та з урахуванням чинних міжнародних зобов'язань. Водночас Протокол не замінює інші угоди, а лише доповнює їх, пропонуючи нові інструменти для більш ефективної боротьби з кіберзлочинністю.

Суттєвим нововведенням Протоколу є закріплення механізмів, які дозволяють уповноваженим органам однієї держави напряму звертатися до провайдерів послуг або реєстраторів доменних імен, що знаходяться на території іншої держави-учасниці, для отримання необхідної інформації. Це стосується, зокрема, відомостей про абонентів або осіб, що зареєстрували доменні імена. Такий підхід значно скорочує строки доступу до даних та мінімізує бюрократичні бар'єри. Водночас постачальники послуг діють у межах національних правових систем і з дотриманням визначених процедур, що забезпечує баланс між потребами слідства та захистом прав суб'єктів.

Отже, запровадження Другого Додаткового протоколу до Будапештської конвенції має вагомe значення і для адміністративного провадження, адже воно створює можливість оперативного та законного отримання цифрових доказів у випадках, коли такі матеріали необхідні для підтвердження або спростування фактів правопорушень. Використання встановлених процедур і міжнародних механізмів дозволяє не лише забезпечити належний рівень захисту прав учасників адміністративних процесів, а й зміцнити довіру до результатів розгляду справ завдяки підвищенню достовірності й автентичності електронних доказів.

Відомо, що у державах романо-германської правової системи будь-які об'єктивні факти, що здатні підтвердити реальний стан справи, можуть бути прийняті судом, тому навіть у випадках, коли цифрові докази не отримали чіткого законодавчого закріплення, вони все ж можуть використовуватися через більш ліберальні підходи до видів доказів. Натомість для англо-американської правової системи, що орієнтована на суворе регулювання доказової бази, найвищу доказову цінність має оригінал документа, а цифрові копії часто оцінюються судами неоднозначно.

В різних правових традиціях під цифровими доказами розуміють будь-яку інформацію, створену, збережену або передану у цифровій формі, яка може бути залучена для підтвердження або спростування факту, що є предметом судового розгляду [11, с. 11]. Використання цифрових доказів у справах про адміністративні правопорушення стає об'єктивною потребою, оскільки суди повинні адаптуватися до сучасних соціально-економічних змін, зумовлених впровадженням електронних послуг. При цьому необхідно враховувати стандарти поведінки з такими доказами та їхню доказову силу, щоб забезпечити їхнє належне застосування та визнання у судовому процесі. Можна припустити, що розвинені країни досягли значного прогресу у впровадженні цифрових доказів. Проте на практиці більшість досліджуваних держав досі не мають нормативно визначених правил щодо їхнього використання в адміністративному процесі.

Результативність застосування сучасних технічних засобів підтверджується практикою зарубіжних країн. Зокрема, впровадження систем відеоспостереження в державах Європейського Союзу та Сполучених Штатах Америки значно підвищило оперативність реагування правоохоронних органів на правопорушення та дало можливість швидко ідентифікувати осіб, які їх вчинили [12, с. 410].

У Сполучених Штатах Америки функціонують Федеральні правила доказів (Federal Rules of Evidence) [13], які встановлюють порядок представлення доказів виключно у цивільних та кримінальних справах у федеральних судах США. Починаючи з 2006 року, у всіх федеральних судах почала діяти оновлена редакція Федеральних правил цивільного судочинства (Federal Rules of Civil Procedure), що надає електронним документам та паперовим рівноцінний правовий статус [14]. Це означає, що будь-яка інформація, збережена в електронному форматі, може бути використана як доказ у відповідності до цих норм.

Одним із ключових напрямів, пов'язаних з інститутом доказування у цифровій сфері, виступає адміністративно-юрисдикційна діяльність органів публічної влади. Так, забезпечення дотримання Правил дорожнього руху та застосування адміністративних заходів до правопорушників покладено на Національну поліцію України. Для належного виконання цих повноважень чинне законодавство передбачає низку інструментів, серед яких – автоматизована система фіксації порушень правил, норм і стандартів, що стосуються безпеки дорожнього руху.

Основна функція цієї системи полягає у реалізації принципу невідворотності покарання, зменшенні корупційних ризиків та мінімізації впливу «людського фактора» під час провадження у справах про адміністративні правопорушення. Хоча законодавець закріпив загальні принципи та процедури притягнення до відповідальності за правопорушення, зафіксовані автоматично, їхня повна практична реалізація ще не була забезпечена. Варто відзначити, що кожна країна має власні особливості у сфері правового регулювання застосування технічних засобів контролю. Саме тому порівняльно-правовий метод дослідження в адміністративному праві дає можливість не лише ознайомитися з положеннями іноземних нормативних актів, але й визначити їхні сильні та слабкі сторони, а також адаптувати найкращі практики для вдосконалення національної правової бази.

Ситуація в європейських країнах у цьому питанні суттєвих відмінностей не має. Так, польське законодавство не виділяє «цифрові докази» як окрему категорію доказів. Жоден із процесуальних кодексів, адміністративний, цивільний чи кримінальний, не містить такого визначення або його аналогу. Доказами визнається будь-яка інформація, що сприяє з'ясуванню обставин справи та не суперечить чинному законодавству (§1 ст. 75 Адміністративно-процесуального кодексу Республіки Польща) [15]. При цьому надані докази в Польщі мають бути оформлені відповідно до вимог закону «Про інформатизацію діяльності суб'єктів, що виконують державні завдання», дотримуючись встановленого формату та містячи електронну адресу відправника.

Чеський адміністративно-процесуальний кодекс [16] встановлює основні правила щодо доказів у адміністративному провадженні та містить перелік допустимих доказів. Водночас він регулює лише ті засоби доказування, які прямо зазначені в кодексі (документи, протоколи огляду, свідчення та експертні висновки). Поза цим кодекс мовчить про інші форми доказування та не дає визначення поняттю «доказ».

У спеціальній літературі Чехії підкреслюється, що адміністративні органи нерідко змушені використовувати додаткові засоби доказування, які не врегульовані кодексом, зокрема аудіовізуальні записи або інформацію з веб-сайтів. Попри те, що такі форми доказів усе час-

тіше застосовуються в адміністративному судочинстві, їх правове регулювання залишається недостатнім. Найважливіші норми адміністративно-процесуального права Чехії на них не поширюються. Ця прогалина особливо помітна, оскільки такі докази активно використовуються у справах, що стосуються адміністративних деліктів, захищають права та законні інтереси учасників публічної адміністрації, а також зачіпають ключові принципи демократичного суспільства та верховенства права. Йдеться, з одного боку, про право на справедливий судовий розгляд і недоторканість приватного життя, а з іншого про законні інтереси суспільства та держави у встановленні фактів правопорушень та забезпеченні справедливого покарання [17, с. 132].

Досвід також доводить, що поєднання мобільних перевірок дорожньої поліції зі стаціонарними камерами, зокрема тими, що вимірюють середню швидкість руху або час проходження відстані, є ефективним

інструментом зменшення кількості випадків перевищення швидкості.

**Висновки.** Отже, на сучасному етапі розвитку людства, де цифрові технології пронизують усі сфери суспільного життя, питання використання цифрових доказів набуває особливої ваги. Адміністративно-правові відносини вже давно не обмежуються лише традиційними формами контролю та регулювання, а дедалі більше переходять у цифровий вимір. Це означає, що у справах про адміністративні правопорушення роль доказів, отриманих і зафіксованих за допомогою технічних засобів, стає визначальною. Міжнародні підходи до визначення та застосування таких доказів відображають різні рівні зрілості правових систем, різні традиції правозастосування та різні пріоритети між забезпеченням ефективності правосуддя і захистом прав людини. Саме тому дослідження міжнародного досвіду у цій сфері має велике теоретичне та практичне значення.

#### ЛІТЕРАТУРА

1. Конвенція про кіберзлочинність Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 URL: [https://zakon.rada.gov.ua/laws/show/994\\_575#Text](https://zakon.rada.gov.ua/laws/show/994_575#Text)
2. ISO/IEC 27037:2012 URL: <https://www.iso.org/standard/44381.html>
3. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. URL: <https://eur-lex.europa.eu/eli/reg/2023/1543/oj>
4. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32023L1544>.
5. Criminal Procedure Law of the People's Republic of China. 2012. URL: <https://www.lawinfochina.com/display.aspx?lib=law&id=9247&C-Gid#:~:text=Article%202%20The%20objectives%20of,by%20law%20and%20combating%20crimes%2C>
6. The provisions of the Supreme People's Court of the People's Republic of China, the Supreme People's Procuratorate of the People's Republic of China and the Ministry of Public Security of the People's Republic of China. 2016. URL: <https://splcgk.court.gov.cn/gzfwwww//spyw/spywDetails?id=84ba1d7cbc0540d59fe49341f8b1ef85>.
7. Guidelines for digital forensics first responder. Best practices for search and seizure of electronic and digital evidence. 2021. URL: [https://www.interpol.int/content/download/16243/file/Guidelines to Digital Forensics First Responders\\_V7.pdf](https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf).
8. Kančauskienė, J. Computer forensics and electronic evidence in criminal legal proceedings: Lithuania's experience. *Digital Evidence and Electronic Signature Law Review*, 2019, 16, 11-24. DOI: <https://doi.org/10.14296/deeslr.v16i0.5015>.
9. Другий Додатковий протокол до Конвенції про кіберзлочинність (Будапештської конвенції) URL: <https://rm.coe.int/ru-2ndaddprotocol-cybercrime-amended-nov2021/1680a54ecf>
10. Міжнародні стандарти та правова регламентація цифрових (електронних) доказів у кримінальному аналізі: науково-методичні рекомендації. Х.: ХНУВС, 2024. 36 с.
11. Бакутін Є. І. Світовий досвід в ефективності використання технічних засобів фіксації правопорушень. Світовий досвід підготовки кадрів поліції та його впровадження в Україні: міжнар. наук.-практ. конф. (Дніпропетровськ, 17 берез. 2016 р.). Дніпропетровськ: Дніпроп. Держ. Ун-т внутр. справ, 2016. С. 410–413.
12. Federal Rules of Evidence (01.07.1975). URL: [https://www.uscourts.gov/sites/default/files/federal\\_rules\\_of\\_evidence\\_-\\_december\\_2020\\_0.pdf](https://www.uscourts.gov/sites/default/files/federal_rules_of_evidence_-_december_2020_0.pdf)
13. Federal Rules of Civil Procedure (01.12.2006). United States Rules and Policies. URL: [https://www.uscourts.gov/sites/default/files/federal\\_rules/FRCP12.1.2006.pdf](https://www.uscourts.gov/sites/default/files/federal_rules/FRCP12.1.2006.pdf)
14. Kodeks postępowania administracyjnego z dnia 14 czerwca 1960 r. URL: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19600300168/U/D19600168Lj.p>
15. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 r. URL: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230000057/T/D20230057L.pdf>
16. Code of Administrative Procedure. Zákon č. 500/2004 Sb., správní řád. URL: <https://www.zakonyprolidi.cz/cs/2004-500>
17. Frumarová K. Evidence in administrative proceedings – proof by audio-visual record, proof by the content of the website and other means of proof lacking explicit regulation in the Code of Administrative Procedure. *Institutiones Administrationis. Journal of Administrative Sciences*. Vol. 2 (2022). No. 1, 132–143. DOI: <https://doi.org/10.54201/iajas.v2i1.31>