

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

МОСКОВЧУК ДМИТРО ОЛЕКСАНДРОВИЧ

УДК: 347.94:004-021.272(100)(043.5)

ДИСЕРТАЦІЯ

**ЕЛЕКТРОННІ ДОКАЗИ У КРАЇНАХ
КОНТИНЕНТАЛЬНОГО ТА ЗАГАЛЬНОГО ПРАВА: ПОРІВНЯЛЬНО-
ПРАВОВЕ ДОСЛІДЖЕННЯ**

081 – Право

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Д.О. Московчук

Науковий керівник –

Неллі Юріївна ГОЛУБЄВА,

доктор юридичних наук, професор

Одеса – 2023

АНОТАЦІЯ

Московчук Д.О. Електронні докази у країнах континентального та загального права: порівняльно-правове дослідження. - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право». – Національний університет «Одеська юридична академія», Одеса, 2023.

Дисертація є першим в Україні комплексним науковим дослідженням електронних доказів у цивільному процесуальному праві України та країн континентального й загального права в порівняльно-правовому аспекті.

Встановлено, що електронні докази – це дані (включаючи вихідні дані аналогових пристроїв або дані в електронній формі), які обробляються, зберігаються або передаються будь-яким виготовленим пристроєм, комп'ютером чи комп'ютерною системою або передаються через систему зв'язку, які можуть скласти фактичну інформацію про будь-який факт. Підкреслено, що електронним доказом може бути будь-який електронний файл із цифрового або аналогового джерела. Це включає електронні листи, текстові повідомлення, миттєві повідомлення, файли та документи з жорстких дисків, електронні фінансові операції, аудіофайли та відеофайли тощо.

Побудовано дворівневу модель системи електронних доказів, залежно від особливостей джерел їх отримання та способу використання в процесі судового доказування: перший рівень - електронні докази, які за характеристиками матеріального носія та електронної інформації можуть бути безпосередньо доставлені в судові засідання та досліджені судом без використання спеціальних знань; другий рівень - електронні докази, які або через особливості носія не можуть бути доставлені до суду, або специфіка електронної інформації, яку вони містять, не дозволяє їх дослідження без застосування спеціальних знань.

Доведено автентичність вітчизняного юридичного механізму використання електронної інформації в процесі судового доказування, який характеризується поєднанням поліваріантності джерел отримання та фіксування електронних доказів із використанням традиційних процедур їх дослідження та оцінки;

Обґрунтовано доцільність запозичення наявної в судах країн загального права практики в разі подання до суду паперової копії електронного документа здійснювати роздруківку та подавати до суду не лише основний текст документа, а й метадані, що сприятиме більш повному відображенню паперовою копією фактичних даних з оригіналу електронного документа та зручності сприйняття їх судом;

Стверджується про необхідність більш чіткої регламентації в нормах законодавства значення електронного підпису для юридичної сили електронного доказу.

Удосконалено визначення поняття «цифровий доказ», відповідно до якого цифровий доказ - це вид електронного доказу, який формується або перетворюється в числовий формат і може бути досліджений лише за допомогою ЕОМ;

Розширено перелік ознак електронних доказів та виділено з-поміж інших наступні ознаки: а) значний обсяг доказової інформації може бути отримано з одного джерела; б) простота передачі та копіювання відомостей із одного електронного носія інформації на інший; в) можливість віддаленого доступу до змісту електронного носія та інформаційно-телекомунікаційних систем (зокрема, до мережі Інтернет).

Визначено формулювання однієї з основних ознак електронного доказу, яка характеризує форму його існування, а саме - це такий вид засобу доказування, що містить дані про обставини справи, оригінал якого генерується, обробляється, зберігається та/або передається лише за допомогою електронного пристрою;

Запропоновано внесення змін до ч. 1 ст. 100 ЦПК України щодо електронного доказу, під яким розуміється інформація в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі.

Обґрунтовано критерії відмежування електронних доказів від інших «традиційних» судових доказів, перелік яких пропонується доповнити критерієм науковості, яка є результатом практичних експериментів із застосуванням наукового методу. Цей метод використовується для отримання достовірних даних і фактів, які були представлені для доведення або спростування фактів, що потребує використання високоякісних наукових даних та застосування спеціальних знань технічних фахівців для перевірки достовірності доказів;

Зроблено висновок, що повідомлення, направлене електронною поштою, та не скріплене електронним підписом відправника, на практиці може розглядатися як достовірний доказ лише в разі, якщо відправник не заперечує факту відправлення ним такого повідомлення;

Зроблено висновок, що у США відсутнє чітке розмежування доказів на види, а доказове право згруповано за типовими для практики проблемними ситуаціями. Статутне доказове право США, по суті, є закріпленням найважливіших та знакових судових рішень, узагальненою практикою, і носить, переважно, заборонний характер, тобто вказує, в яких випадках доказ не може бути визнаним допустимим. За таких обставин питання про те, чи є «електронні докази» самостійним видом доказів, немає істотного значення для американських юристів.

Встановлено, що в цивільному процесуальному праві Англії та Уельсу також не виділяється такого окремого виду доказів як електронні докази, у Правилах цивільного судочинства йдеться лише про процедури та правила

подання електронних документів. «Електронний документ» означає будь-який документ, що зберігається в електронній формі: електронна пошта та інші електронні засоби зв'язку, такі як текстові повідомлення і голосова пошта, текстові документи й бази даних, а також документи, що зберігаються на портативних пристроях, таких як карти пам'яті й мобільні телефони. На додаток до документів, які легко доступні з комп'ютерних систем та інших електронних пристроїв і носіїв, включаються документи, які зберігаються на серверах і системах резервного копіювання, і документи, які були видалені. Він також включає метадані та інші вбудовані дані, які зазвичай не видно на екрані або на роздруківці. В англійському праві термін «документ», крім письмових актів, охоплює також: а) карти, плани, графіки чи креслення; б) фотографії; в) диски, стрічки, звукові доріжки, інші пристрої, за допомогою яких звуки зафіксовані й можуть бути відтворені; г) фільми, негативи, що закріпили зорові образи та здатні їх відтворювати. Підкреслено, що розрізняються поняття «електронне зображення» паперового документа та «власне електронний документ» - електронний документ, що зберігається у вихідній формі, в якій він був створений за допомогою комп'ютерної програми. Копіями документів називаються також копії магнітофонних записів, репродукції зображень і т.д.

Стверджується, що розвиток електронних доказів у Франції тісно пов'язаний з електронним підписом та електронними листами, оскільки швидка поява нових комунікаційних засобів та інтенсивне використання Інтернету викликали необхідність адаптації законодавства Франції до сучасних потреб. Доведено, що протягом тривалого часу письмові докази були синонімом паперових доказів, пізніше законодавець вирішив розв'язати цю проблему. Тому було вирішено, що необхідно встановити визначення письмових доказів, яке включатиме як традиційні, так і електронні письмові документи.

Вказано, що в німецькій процесуальній літературі під електронним документом прийнято розуміти текстові, аудіо-, відео- та програмні

документи. Така думка ґрунтується на віднесенні електронного документа до речових доказів, і, відповідно, розумінні його як файлу, який може бути записаний на носії інформації. У цивільному процесі Німеччини загальні вимоги, що пред'являються до речових доказів, прийнято застосовувати і до електронних документів.

Проаналізовано визначення електронного документа в Італії, викладене наступним чином: «комп'ютерний документ: інформаційне відображення дій, фактів або юридично релевантних даних». Обґрунтовано, що це визначення недостатньо детальне, проте з деякими корективами воно посилається на традиційне визначення документа. Також невід'ємною складовою електронного документа за законодавством Італії є електронний підпис, який надає такому документу юридичної сили. Електронний підпис - це набір даних в електронній формі, доданих або логічно пов'язаних з іншими електронними даними, що використовуються як спосіб ідентифікації.

Досліджено закріплений в італійському законодавстві принцип еквівалентності паперових та електронних документів, відповідно до якого електронний документ, підписаний цифровим підписом, прирівнюється за юридичною силою до документа з рукописним підписом. При цьому саме власник підписного пристрою вважається підписантом електронного документа, якщо він не доведе протилежного.

Доведено розбіжність у правовій регламентації правил щодо електронних доказів між Україною та іншими державами полягає у видовій належності електронних доказів. Так, наприклад, до речових доказів відносить електронні документи Цивільний процесуальний кодекс Німеччини, а у Франції та Італії електронні документи розглядають як письмові докази. Верховна рада України під час розробки та ухвалення нової редакції ЦПК прийняла концепцію, згідно якої електронні докази розглядаються як окремий вид засобу доказування.

Зроблено висновок, що ще однією відмінністю є те, що норми ЦПК України дозволяють проведення огляду електронних доказів за їх

місцезнаходженням у разі неможливості їх доставлення. Для правозастосування в США, наприклад, використовуються науковці та технічні фахівці для надання достовірних даних і фактів, які були представлені для доведення або спростування фактів, що мають значення для справи. У Франції ж доказова цінність електронної пошти може бути відновлена за допомогою судового виконавця та за допомогою комп'ютерного експерта, який зазначав би наявність електронних листів на сервері особи, яка заперечує їх існування або автентичність.

Ключові слова: суд, докази, доказування, інформаційні технології, електронні докази, електронний документ, електронне судочинство, діджиталізація, цивільний процес, зарубіжний досвід.

ABSTRACT

Moskovchuk D.O. Electronic evidence in continental and common law countries: a comparative legal study. – *Qualifying scientific work as a manuscript.*

Thesis for the degree of Doctor of Philosophy in the field of knowledge 08 «Law» in specialty 081 «Law». – National university «Odesa Law Academy», Odesa, 2023.

The dissertation is the first comprehensive scientific study of electronic evidence in the civil procedural law of Ukraine and continental and common law countries in a comparative legal aspect.

Electronic evidence is defined as data (including the output of analog devices or data in electronic form) processed, stored, or transmitted by any manufactured device, computer, or computer system, or transmitted through a communications system, that can compile factual information about any fact. It is emphasized that electronic evidence can be any electronic file from a digital or analog source. This includes e-mails, text messages, instant messages, files and

documents from hard drives, electronic financial transactions, audio and video files, and others.

A two-level model of the electronic evidence system has been worked out, depending on the specifics of the sources of their receipt and the method of use in the process of judicial evidence: the first level – electronic evidence, which, according to the characteristics of the physical medium and electronic information, can be directly delivered to the court session and examined by the court without the use of special knowledge; the second level – electronic evidence, which either due to the peculiarities of the medium cannot be delivered to the court, or the specifics of the electronic information they contain does not allow their research without the use of special knowledge.

The authenticity of the domestic legal mechanism for the use of electronic information in the process of judicial evidence is proven, which is characterized by a combination of multivariate sources of obtaining and recording electronic evidence with the use of traditional procedures of their research and evaluation;

The research substantiates the expediency of borrowing the practice available in the courts of common law countries in the case of submitting a paper copy of an electronic document to the court to make a printout and submit to the court not only the main text of the document, but also the metadata, which will contribute to a more complete reflection of the actual data from the original electronic document in the paper copy and to the convenience of their perception by the court;

It is asserted that there is a need for a clearer regulation in the legislation of the meaning of an electronic signature for the legal force of an electronic proof.

The definition of the concept of «digital evidence» has been improved, according to which digital evidence is a type of electronic evidence that is formed or converted into a numerical format and can be examined only with the help of a computer;

The list of features of electronic evidence has been expanded and the following features have been highlighted among others: a) a significant amount of

evidentiary information can be obtained from one source; b) ease of transferring and copying information from one electronic medium to another; c) the possibility of remote access to the content of electronic media and information and telecommunication systems (in particular, to the Internet).

The definition of one of the main features of electronic evidence, which characterizes the form of its existence, is determined, namely, it is a type of evidence that contains data about the circumstances of the case, the original of which is generated, processed, stored and/or transmitted only by means of an electronic device;

The work offers amendments to Part 1 of Art. 100 of the Civil Procedure Code of Ukraine regarding electronic evidence, which means information in electronic (digital) form containing data on circumstances relevant to the case in electronic form. Such data can be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, other places of data storage in electronic form.

The criteria for distinguishing electronic evidence from other «traditional» court evidence are substantiated, the list of which is proposed to be supplemented with the criterion of scientificity, which is the result of practical experiments using the scientific method. This method is used to obtain reliable data and facts that have been presented to prove or disprove the facts, which requires the use of high-quality scientific data and the application of special knowledge of technical specialists to verify the reliability of the evidence;

It has been concluded that a message sent by e-mail and not sealed with an electronic signature of the sender can in practice be considered as reliable evidence only if the sender does not deny the fact of sending such a message;

It has been concluded that in the USA there is no clear division of evidence into types, and evidentiary law is grouped according to typical problematic situations for practice. The statutory evidentiary law of the USA, in fact, is a consolidation of the most important and landmark court decisions, a generalized practice, and is mainly of a prohibitive nature, that is, it indicates in which cases

the evidence cannot be recognized as admissible. Under such circumstances, the question of whether «electronic evidence» is an independent type of evidence is of no significant importance to American lawyers.

It has been established that the civil procedural law of England and Wales also does not distinguish such a separate type of evidence as electronic evidence, the Rules of Civil Procedure refer only to the procedures and rules for submitting electronic documents. An «electronic document» means any document stored in electronic form: e-mail and other electronic means of communication, such as text messages and voice mail, text documents and databases, as well as documents stored on portable devices, such as memory cards and mobile phones. In addition to documents that are readily accessible from computer systems and other electronic devices and media, this includes documents stored on servers and backup systems and documents that have been deleted. It also includes metadata and other embedded data that is not normally visible on screen or in a printout. In English law, the term «document» includes, in addition to written acts: a) maps, plans, graphs or drawings; b) photographs; c) disks, tapes, sound tracks, other devices, with the help of which sounds are recorded and can be reproduced; d) films, negatives that fixed visual images and are capable of reproducing them. It is emphasized that there are differences between the concepts of «electronic image» of a paper document and an «electronic document proper» – an electronic document stored in the original form in which it was created using a computer program. Copies of documents are also called copies of tape recordings, reproductions of images, etc.

It is argued that the development of e-evidence in France is closely related to e-signatures and e-mails, as the rapid emergence of new means of communication and the intensive use of the Internet have necessitated the adaptation of French legislation to modern needs. It has been proven that for a long time written evidence had been synonymous with paper evidence, later the legislator decided to solve this problem. It was therefore decided that a definition of written evidence should be established which would include both traditional and

electronic written documents.

It is indicated that in the German procedural literature, an electronic document is understood as text, audio, video and software documents. This opinion is based on the classification of an electronic document as material evidence, and, accordingly, understanding it as a file that can be recorded on an information carrier. In the German civil process, the general requirements for material evidence are also applied to electronic documents.

The definition of an electronic document in Italy has been analyzed, which is stated as follows: «computer document: information display of actions, facts or legally relevant data». It is substantiated that this definition is not detailed enough, but with some corrections it refers to the traditional definition of a document. Also, an integral component of an electronic document under Italian law is an electronic signature, which gives such a document legal force. An electronic signature is a set of data in electronic form, added or logically connected to other electronic data, used as a means of identification.

The principle of equivalence of paper and electronic documents secured in Italian legislation has been studied, according to which an electronic document signed with a digital signature is equal in legal force to a document with a handwritten signature. At the same time, it is the owner of the signature device who is considered the signatory of the electronic document, unless he proves otherwise.

It has been proven that the discrepancy in the legal regulation of rules regarding electronic evidence between Ukraine and other states lies in the type of electronic evidence. For example, the German Civil Procedure Code includes electronic documents as material evidence, and in France and Italy electronic documents are considered as written evidence. The Verkhovna Rada of Ukraine, during the development and adoption of the new edition of the Civil Procedure Code, adopted the concept according to which electronic evidence is considered as a separate type of means of proof.

It has been concluded that another difference is that the norms of the Civil Procedure Code of Ukraine allow the review of electronic evidence based on their location in case of impossibility of their delivery. Law enforcement in the US, for example, uses scientists and technicians to provide reliable data and facts that have been presented to prove or disprove facts relevant to the case. In France, the probative value of e-mail can be restored with the help of a bailiff and with the help of a computer expert, who would note the presence of e-mails on the server of a person who denies their existence or authenticity.

Key words: court, evidence, proving, information technology, electronic evidence, electronic document, electronic judicial proceedings, digitalization, civil process, foreign experience.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації, в яких опубліковані основні наукові результати дисертації:

1. Московчук Д.О. Порівняльний аналіз законодавства України та країн англо-саксонської правової системи щодо подання доказів у цивільному процесі. *Підприємництво, господарство і право*. 2019. №4 (278) С. 55-60.
2. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Індія. *Юридичний науковий електронний журнал*. 2022. №7/22. С. 559-562.
3. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Узбекистан. *Право та державне управління*. 2022. №2. С. 304-308.
4. Московчук Д.О. Кіліміченко А.О. Загальна характеристика допустимості та достовірності електронних доказів у законодавстві Малайзії та Республіки Сінгапур. *Часопис цивілістики*. 2021. № 41. С. 66-70.

Публікації, які засвідчують апробацію матеріалів дисертації:

1. Московчук Д.О., Даниляк Р.П. Загальна характеристика електронних доказів у законодавстві Сінгапуру. *Сучасна цивілістика: 15 років наукових звершень* : матеріали XV Міжнародної науково-практичної конференції, (м. Одеса, 22 трав. 2020 р.) Одеса, 2020. С. 364-365
2. Московчук Д.О. Загальна характеристика електронних доказів США та Німеччини. *Реформування цивільного процесуального права в умовах інтеграційних процесів в Україні* : матеріали Всеукраїнської науково-практичної інтернет-конференції ім. Ю.С. Червоного, (м. Одеса, 18 грудня. 2020 р.) Одеса, 2020. С. 37-39.
3. Московчук Д. О. Обмеження щодо подання електронних доказів у законодавстві США. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)* : у 2 т. : матеріали Міжнародної науково-практичної конференції, (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса: Видавничий дім «Гельветика», 2022. Т. 2. С. 801-803.
4. Московчук Д.О. Питання щодо особливостей електронних доказів у цивільному процесі Республіки Узбекистан. *Цивільне судочинство та виконавче провадження в умовах воєнного стану* : матеріали Всеукраїнської науково-практичної конференції ім. Ю. С. Червоного, (Одеса, 16 грудня 2022 р.) [Електронне видання] / за заг. ред. Н. Ю. Голубевої. Одеса : Фенікс, 2022. С. 47-49.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	3
ВСТУП.....	4
РОЗДІЛ 1. МЕТОДОЛОГІЧНІ ТА КОНЦЕПТУАЛЬНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У ЗАРУБІЖНИХ КРАЇНАХ.....	15
1.1. Методологія та вибір напрямів дослідження.....	15
1.2. Вплив глобалізації та науково-технічного прогресу на формування системи джерел електронних доказів.....	23
1.3. Поняття та види електронних доказів у цивільному судочинстві.....	46
РОЗДІЛ 2. ЕЛЕКТРОННІ ДОКАЗИ В ЦИВІЛЬНОМУ СУДОЧИНСТВІ КРАЇН АНГЛО-АМЕРИКАНСЬКОЇ ПРАВОВОЇ СІМ'Ї.....	71
2.1. Практико-орієнтований підхід до електронних доказів у цивільному судочинстві США.....	71
2.2. Консервативний підхід до електронних доказів у цивільному судочинстві Великобританії.....	90
РОЗДІЛ 3. ЕЛЕКТРОННІ ДОКАЗИ В ЦИВІЛЬНОМУ СУДОЧИНСТВІ КРАЇН РОМАНО-ГЕРМАНСЬКОЇ ПРАВОВОЇ СІМ'Ї.....	106
3.1. Місце електронних документів у системі судових доказів у цивільному судочинстві Французької Республіки.....	106
3.2. Сутність та доказова сила електронних доказів за законодавством та правовою доктриною Федеративної Республіки Німеччина.....	120
3.3. Принцип еквівалентності паперових та електронних документів у законодавстві Італійської Республіки.....	146
ВИСНОВКИ.....	161
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	168
ДОДАТКИ.....	190

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ:

ЕОМ – електро-обчислювальна машина

ЄС – Європейський Союз

ІТ – інформаційні технології, інформаційно-телекомунікаційні технології

КЦУ – Кодекс цифрового управління Італійської Республіки

ОЗП – оперативний запам'ятовувальний пристрій

ПВ – Практичні вказівки для судів Англії

ПЗП – постійний запам'ятовувальний пристрій

ПЦС – Правила цивільного судочинства Англії

ЦК Італії – Цивільний кодекс Італійської Республіки

ЦК Франції – Цивільний кодекс Французької Республіки

ЦПК Італії – Цивільний процесуальний кодекс Італійської Республіки

ЦПК України – Цивільний процесуальний кодекс України

ЦПК Франції – Цивільний процесуальний кодекс Французької Республіки

ЦПК ФРН – Цивільний процесуальний кодекс Федеративної Республіки

Німеччина

ВСТУП

Правові системи формуються поступово під впливом різних політичних та історико-культурних чинників, що відображається практично на всіх галузях права, зокрема й таких як цивільне процесуальне право. Скільки століть існували держава та право, стільки ж століть людство працювало над виробленням найбільш ефективної моделі вирішення юридичних спорів.

Відокремлений розвиток правових систем був спричинений різноманітними економічними, географічними, політичними та іншими факторами. Однак у сучасному світі відокремлений розвиток неможливий через ті самі фактори, які стали по-іншому впливати на розвиток права, що рухається від відособленого розвитку правових систем до їх зближення, уніфікації багатьох норм та процедур.

Конвергенція правових систем часом призводить до формування єдиного правового простору, як це відбулося в Європейському Союзі, коли ціла низка країн, що мають спільні цінності, намагаються поступово сформувати єдину європейську правову систему, яка існує паралельно з правовими системами країн-членів та поступово впливає на їх розвиток та подальше зближення. В умовах євроінтеграційних прагнень України неможливо обійтися без використання зарубіжного досвіду для розвитку оптимальної для теперішнього часу процедури, яка була б здатна захистити порушені права та охоронювані законом інтереси суб'єктів правовідносин.

Без вивчення зарубіжного права сьогодні немислимий розвиток національних правових систем та навіть будь-якої галузі права, що є проявом загальної тенденції до глобалізації та посилення інтеграційних процесів у суспільстві.

По-перше, різні прояви інтеграції країн призводять до економічного, політичного, правового зближення та співробітництва. Очевидно, що запозичення правового досвіду тих країн, де відповідні правові інститути

мають довшу історію розвитку та сприяють більш ефективному регулюванню суспільних відносин, просто неминуче. Мова може йти про сприйняття цілих галузей права, що відбувалося в деяких країнах, або про запозичення окремих інститутів, юридико-технічних засобів, певних концепцій, ідей і т.ін.

У межах даного дисертаційного дослідження інтерес представляє саме зарубіжний досвід використання електронних доказів у процесі судового доказування, зокрема законодавчий і правозастосовний досвід розвинених країн англо-американської та романо-германської правових сімей, таких як США, Великобританія, Французька Республіка, Федеративна Республіка Німеччина, Італійська Республіка, які мають яскраво виражені ознаки належності до певної правової сім'ї, та, де положення про електронні докази вже стали невід'ємною складовою доказового права й доволі активно та ефективно використовуються в судовій практиці, а отже, є перспективними для наукового аналізу та вивчення можливостей запозичення їх позитивного досвіду.

По-друге, суди різних країн змушені застосовувати норми міжнародного права та оцінювати процесуальні результати дій, вчинених на підставі норм права іншої країни. Так, виконання судових доручень, збирання доказів, виконання рішень іноземних судів на території України може потребувати ознайомлення із правовою системою тієї чи іншої країни.

По-третє, вивчення зарубіжного права забезпечує знайомство з теорією права, ідеями, поняттями, концепціями, притаманними іншим правовим системам.

Відомо, що у світі склалося дві основні моделі судового процесу: інквізиційна (слідча) та змагальна. Елементи першої моделі частіше можна зустріти в судочинстві країн романо-германської правової сім'ї, чия правова система історично сформувалася під впливом римського права, тоді як у країнах загального права змагальність проявляється в більш чистому вигляді. У зв'язку з цим мова йтиме про особливості романо-германського та

загального права, що дали життя різним системам цивільного процесу й досі визначають напрями подальшої еволюції правосуддя, зокрема, й у питанні використання електронних доказів у процесі судового доказування.

Роль та значення інформаційних технологій для існуючих суспільних відносин, у тому числі й цивільних процесуальних правовідносин, досить велика та постійно зростає. Фізичні та юридичні особи у своїй повсякденній діяльності активно користуються різними електронними носіями інформації. Таке використання пов'язане із зберіганням, передачею, переробкою та іншими видами використання значних масивів електронної інформації, яка нерідко використовується як доказ у судових процесах. Саме потреба в унормування такого використання призвела до того, що в Законі України від 03.10.2017 «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів», яким було викладено в новій редакції ЦПК України, ГПК України та КАС України, в процесуальні кодекси були внесені норми, що містять уніфіковані положення щодо доказів у адміністративному, господарському та цивільному процесах, а також запроваджено новий вид засобу доказування – електронний доказ.

Наявність значної кількості складнощів, помилок та неоднозначного трактування положень процесуального закону в судовій практиці спричиняє необхідність вдосконалення вчення про електронні докази в цивільному судочинстві, зокрема й шляхом запозичення іноземного досвіду в цій сфері.

Вагомий внесок у розробку наукових положень щодо електронних доказів в Україні та за кордоном здійснили такі вітчизняні науковці-правники: О.І. Антонюк, І.С. Апалькова, О.О. Воронюк, М.О. Гетманцев, Н.Ю. Голубєва, К.Б. Дрогозюк, С.В. Дяченко, І.М. Іліопол, А.Ю. Каламайко, О.М.Лазько, Ю.С. Павлова, В.С. Петренко, О.Ю. Поклонська, О.О. Полуніна, Т.В. Степанова, Т.А. Стоянова, Ю.Ю. Цал-Цалко, Д.М. Цехан, С.А. Чванкін, О.С. Чорний, А.С. Штефан та ін.

Крім вітчизняних правників, дослідженням проблематики електронних доказів займалась значна кількість іноземних науковців, серед яких можна виділити таких: С. Теппер (C. Tapper), Р. Крос (R. Cross), Н. Вілкінс (N. Wilkins), П. Еліот (P. Elliot) та інші.

В Україні протягом тривалого часу проблематиці електронних доказів не приділялося достатньо уваги й лише останнім часом з'явилося декілька дисертаційних досліджень. Серед них А. Ю. Каламайко «Електронні засоби доказування в цивільному процесі» (2016 р.), Ю. С. Павлова «Електронний документ як джерело доказів у цивільному процесі» (2019 р.), С. А. Чванкін «Інформаційні технології у доказуванні в цивільному процесі: теоретичні та практичні аспекти» (2021 р.). Не применшуючи наукових здобутків зазначених науковців, варто, водночас, відзначити, що ними, переважно, був зроблений акцент саме на українському законодавстві та судовій практиці. Порівняльна складова у вказаних дослідженнях хоча й присутня, однак є недостатньо вираженою. Зарубіжний досвід використано доволі фрагментарно, що не дає можливість отримати цілісного уявлення про законодавство та практику розвинених країн у сфері використання електронних доказів у цивільному судочинстві.

Викладені обставини й зумовлюють актуальність теми дисертаційного дослідження, коло досліджених у ньому питань та схему їх висвітлення.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертація підготовлена відповідно до плану науково-дослідної роботи кафедри цивільного процесу Національного університету «Одеська юридична академія» «Реформа цивільного процесуального права в умовах інтеграційних процесів в Україні» на 2016-2020 роки як складової плану науково-дослідної роботи Національного університету «Одеська юридична академія» «Стратегія інтеграційного розвитку України: правовий та культурний вимір» на 2016–2020 рр. (державний реєстраційний номер 0116U001842), а також плану науково-дослідної роботи кафедри цивільного

процесу Національного університету «Одеська юридична академія» «Захист прав людини в порядку цивільного судочинства в цифрову еру» на 2021-2025 рр. як складової плану науково-дослідної роботи Національного університету «Одеська юридична академія» «Правове та соціальне життя людини в людиноцентристському вимірі в цифрову еру» на 2021–2025 рр. (державний реєстраційний номер 0122U000266).

Мета й завдання дослідження. Метою наукового дослідження є здійснення порівняльно-правового аналізу положень законодавства та доктрини права в Україні та іноземних країнах, вивчення можливостей вдосконалення вітчизняної моделі використання електронних доказів у процесі судового доказування шляхом запозичення позитивного закордонного досвіду.

Для досягнення мети дослідження поставлені такі основні завдання:

- визначити сутність та правову природу електронних доказів у цивільному процесуальному праві країн континентального та загального права;
- охарактеризувати різновиди електронних доказів, процесуальні особливості їх використання в цивільному судочинстві країн континентального та загального права;
- зіставити джерела правового регулювання, принципи, правові інститути, пов'язані з використанням електронних доказів у процесі судового доказування в цивільному судочинстві країн загального та континентального права;
- встановити особливості використання електронних доказів у цивільному процесі в країнах англо-американської правової сім'ї;
- дослідити наукові погляди на сутність електронних доказів та особливості правового регулювання їх використання в судовому процесі в країнах романо-германської правової сім'ї;

- розкрити сутність електронного документа й електронного підпису, визначити їх доказове значення за законодавством країн континентального та загального права;

- на основі судової практики виявити проблемні моменти застосування електронних доказів у цивільному процесі країн загального та континентального права;

- визначити основні спільні та відмінні риси електронних доказів за законодавством країн континентального та загального права;

- сформулювати пропозиції щодо вдосконалення положень вітчизняного законодавства шляхом запозичення позитивного досвіду використання електронних доказів у країнах континентального та загального права.

Об'єктом дослідження є суспільні відносини, що виникають під час використання електронних доказів у цивільному процесі в країнах континентального та загального права.

Предметом дослідження є електронні докази у країнах континентального та загального права.

Методи дослідження. Методологічною основою дослідження є діалектико-матеріалістичний метод наукового пізнання соціально-правових явищ і загальнонаукові та спеціальні методи, що базуються на ньому.

Так, *методи формальної логіки* (аналіз, синтез, індукція, дедукція, аналогія та інші) використовувалися в дослідженні нормативних актів, матеріалів судових справ, концепцій, точок зору авторів з окремих питань, що входять до предмета дослідження, їх узагальненні та формулюванні висновків (розділи 1, 2, 3); *моделювання* - під час формування висновків до розділів і загальних висновків у роботі (розділи 1, 2, 3); *описово-аналітичний* - для тлумачення юридичних правових категорій, формулювання дефініцій і уточнення понятійно-категоріального апарату (розділи 1, 2, 3); *порівняльно-правовий метод* - під час співставлення наукових досліджень та концепцій, наявних у вітчизняній та зарубіжній науці, положень нормативних актів

(розділ 2, 3); за допомогою *соціологічного та статистичного методів* проводився аналіз та узагальнення емпіричної бази (розділи 1, 2, 3).

Теоретичну основу дисертаційного дослідження становлять праці вітчизняних і зарубіжних вчених переважно в галузях цивільного процесуального та цивільного права.

Нормативно-правову базу дослідження складають Конституція України, Цивільний процесуальний кодекс України, рішення Верховного Суду, цивільне процесуальне законодавство України, а також законодавство і судова практика окремих країн континентального та загального права.

Наукова новизна одержаних результатів полягає в тому, що дисертація є першим в Україні комплексним науковим дослідженням електронних доказів у цивільному процесуальному праві України та країн континентального й загального права у порівняльно-правовому аспекті.

У результаті дослідження одержано такі результати, що мають наукову новизну:

уперше:

побудовано дворівневу модель системи електронних доказів, залежно від особливостей джерел їх отримання та способу використання в процесі судового доказування: перший рівень - електронні докази, які за характеристиками матеріального носія та електронної інформації можуть бути безпосередньо доставлені в судові засідання та досліджені судом без використання спеціальних знань; другий рівень - електронні докази, які або через особливості носія не можуть бути доставлені до суду, або специфіка електронної інформації, яку вони містять, не дозволяє їх дослідження без застосування спеціальних знань;

доведено автентичність вітчизняного юридичного механізму використання електронної інформації в процесі судового доказування, який характеризується поєднанням поліваріантності джерел отримання та фіксування електронних доказів з використанням традиційних процедур їх дослідження та оцінки;

обґрунтовано доцільність запозичення наявної в судах країн загального права практики в разі подання до суду паперової копії електронного документа здійснювати роздруківку та подавати до суду не лише основний текст документа, а й метадані, що сприятиме більш повному відображенню паперовою копією фактичних даних з оригіналу електронного документа та зручності сприйняття їх судом;

стверджується про необхідність більш чіткої регламентації в нормах законодавства значення електронного підпису для юридичної сили електронного доказу;

удосконалено:

визначення поняття «цифровий доказ», відповідно до якого цифровий доказ - це вид електронного доказу, який формується або перетворюється в числовий формат і може бути досліджений лише за допомогою ЕОМ;

формулювання однієї з основних ознак електронного доказу, яка характеризує форму його існування, а саме - це такий вид засобу доказування, що містить дані про обставини справи, оригінал якого генерується, обробляється, зберігається та/або передається лише за допомогою електронного пристрою;

поняття електронного доказу, під яким розуміється інформація в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи в електронній формі. Такі дані можуть зберігатися, зокрема на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі. Та запропоновано внесення відповідних змін до ч. 1 ст. 100 ЦПК України;

набули подальшого розвитку:

критерії відмежування електронних доказів від інших «традиційних» судових доказів, перелік яких пропонується доповнити критерієм науковості, яка є результатом практичних експериментів із застосуванням наукового методу. Цей метод використовується для отримання достовірних даних і

фактів, які були представлені для доведення або спростування фактів, що потребує використання високоякісних наукових даних та застосування спеціальних знань технічних фахівців для перевірки достовірності доказів;

висновок, що повідомлення, направлене електронною поштою, та не скріплене електронним підписом відправника, на практиці може розглядатися як достовірний доказ лише в разі, якщо відправник не заперечує факту відправлення ним такого повідомлення;

розуміння закріпленого в італійському законодавстві принципу еквівалентності паперових та електронних документів, відповідно до якого електронний документ, підписаний цифровим підписом, прирівнюється за юридичною силою до документа з рукописним підписом. При цьому саме власник підписного пристрою вважається підписантом електронного документа, якщо він не доведе протилежного.

Практичне значення одержаних результатів полягає в тому, що висновки та пропозиції, сформульовані в дисертаційному дослідженні, можуть бути використані в:

- науково-дослідній сфері - як підґрунтя для подальшого розвитку вчення про електронні докази в цивільному процесуальному праві;
- практичній діяльності - для організаційно-методичного та інформаційного забезпечення діяльності суддів, адвокатів та інших практикуючих юристів;
- навчальному процесі - при викладанні дисципліни «Цивільний процес» для підготовки фахівців юридичного профілю у вищих навчальних закладах, підготовці підручників, навчальних та навчально-методичних посібників, курсів лекцій, практикумів із зазначеної дисципліни (акт про впровадження розробок дисертаційного дослідження в освітній процес Національного університету «Одеська юридична академія» від «05» грудня 2022 року; акт про впровадження розробок дисертаційного дослідження в процес підготовки працівників Південного міжрегіонального управління Міністерства юстиції (м. Одеса) від «07» грудня 2022 року);

- законотворчій діяльності - для вдосконалення чинного цивільного процесуального законодавства України та законодавства зарубіжних країн щодо визначення поняття, сутності та порядку використання в процесі судового доказування електронних доказів.

Апробація результатів дисертації. Дисертація підготовлена на кафедрі цивільного процесу Національного університету «Одеська юридична академія». Результати дисертаційного дослідження обговорювалися на засіданнях кафедри цивільного процесу Національного університету «Одеська юридична академія». Основні положення дисертації оприлюднені на 4 міжнародних та всеукраїнських науково-практичних конференціях, круглих столах: XV Міжнародній науково-практичній конференції «Сучасна цивілістика: 15 років наукових звершень» (м. Одеса, 22 травня 2020 р.); Всеукраїнській науково-практичній інтернет-конференції ім. Ю.С. Червоного «Реформування цивільного процесуального права в умовах інтеграційних процесів в Україні» (м. Одеса, 18 грудня 2020 р.); Міжнародній науково-практичній конференції «Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)» (м. Одеса, 17 червня 2022 р.); Всеукраїнській науково-практичній конференції ім. Ю.С. Червоного «Цивільне судочинство та виконавче провадження в умовах воєнного стану» (Одеса, 16 грудня 2022 р.).

Публікації. Основні положення і висновки, що були сформульовані в дослідженні, знайшли відображення у восьми наукових публікаціях, серед яких чотири статті - у виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, а також у чотирьох тезах, опублікованих у збірниках тез доповідей на науково-практичних конференціях.

Структура дисертації. Дисертація складається із вступу, трьох розділів, що містять у собі вісім підрозділів, висновків, списку використаних джерел (236 найменування на 22 сторінках) та двох додатків (на 9 сторінках). Повний обсяг дисертації становить 198 сторінок, з них основний текст - 167 сторінок.

РОЗДІЛ 1. МЕТОДОЛОГІЧНІ ТА КОНЦЕПТУАЛЬНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У ЗАРУБІЖНИХ КРАЇНАХ

1.1. Методологія та вибір напрямку дослідження

Важливим етапом здійснення будь-якої наукової роботи є обрання системи методів, прийомів та підходів до вивчення обраного предмету дослідження, що дозволить найбільш ефективно досягти поставленої дослідницької мети, адже, як справедливо відзначив М. Кравчук, «фундаментальною основою науковості, базовим інструментарієм пізнання юриспруденції є методологія» [32, с. 117]. Адже в наукових джерелах робиться наголос на тому, що сучасна наука може розглядатися як така діяльність з виробництва й організації об'єктивного, достовірного, перевіреного, обґрунтованого тощо знання, що історично виникає у конкретній соціокультурній ситуації, розробляє власні методи й засоби. У цьому розумінні наукою визнається не усяка раціонально організована пізнавальна діяльність, а тільки та, яка здійснюється за певними правилами, засобами й методами, що дають змогу характеризувати вироблені знання як об'єктивні, достовірні, такі, що підлягають перевірці, обґрунтовані тощо» [28, с. 65].

Науковці вказують, що «методологія юриспруденції – результат дискурсу, в межах якого здійснюється процес взаємодії різноманітних когнітивних стратегій осягнення права, визначаються фундаментальні методологічні засади його пізнання. Вона є єдністю трьох взаємозалежних частин – доктринально-ідеологічної, стратегічної та інструментальної. Першу з них можна розглядати як парадигму дослідницького бачення права, тобто тип праворозуміння. Друга – це царина підходів, що зумовлюють загальну спрямованість дослідження права, вибір стратегії його осягнення. Третя частина є системою когнітивних практик, своєрідним набором

методологічних інструментів у створенні знань про право» [21, с.41]. Саме третя складова методології юридичної науки, переважно, окреслена у даному підрозділі.

Сучасна методологія юридичної науки знаходиться на посткласичному (постмодерністському) етапі свого розвитку. Як писав Ю.М. Оборотов, «звертання до постмодерністської методології визначається неможливістю пояснити багато проблем правового й державного життя, керуючись підходами класичної і некласичної методології. Більше того, найчастіше важко усвідомити й інтерпретувати правові та державні реалії не тільки в рамках використання якого-небудь одного методу, а потрібне сполучення методологічних підходів і навіть об'єднання положень класичної, некласичної і постмодерністської методології для вирішення виникаючих політичних і правових проблем» [46, с.41].

Натепер методологія юриспруденції за своєю сутністю є плюралістичною, характеризується взаємодією різноманітних підходів. Варто цілковито підтримати позицію П. Рабіновича, відповідно до якої на зміну світоглядно-філософському монізму радянського періоду сформувався плюралізм таких підходів і концепцій [58, с. 13].

Водночас, відмова від діалектичного матеріалізму як єдино можливого та нав'язаного державною ідеологією методу наукового дослідження не означає цілковитої відмови від діалектичного методу наукового пізнання, який за влучним висловом М. Панова є загальним й універсальним методом формування правових понять, що включає, як відомо, необхідні та вельми важливі етапи сходження від абстрактного до конкретного, і далі, – від конкретного до абстрактного [50, с. 52].

Важливу роль під час даного дослідження відігравало використання правил формально-логічного мислення, аналогії, аналізу й синтезу, наукового узагальнення та ін. Як відзначається науковцями, «усі вони спрямовані на одержання узагальнених і в той же час фундаментальних (істотних) знань про об'єкт дослідження. У результаті абстрагування одне й

те саме судження про найбільш істотні властивості (ознаки) об'єкта або явища державно-правового характеру завжди має бути визначено у відповідних поняттях чи категоріях з необхідною точністю, граничною чіткістю і за допомогою адекватних лінгвістичних компонентів, тобто системи взаємопов'язаних рядів слів (термінів), розташованих у строго логічному порядку стосовно об'єкта пізнання, і однозначно відображати його сутність» [50, с.52].

У рамках даного дослідження важливим є цивілізаційний підхід до вивчення правових явищ і процесів. Як справедливо відзначається в науковій літературі, «цивілізаційний підхід дозволяє визнати природним розмаїття правових культур і державних інститутів як мозаїку світу, що розвивається, зберегти власну унікальність, використовувати досягнення різних цивілізацій, вести з ними культурний діалог, знаходити спільні правові рішення і організаційні засоби їх здійснення при взаємодії з іншими правовими системами і державами» [46, с. 42].

Центральним методом наукового дослідження з огляду на особливості предмета даного дисертаційного дослідження, є порівняльно-правовий метод, сутність якого пояснюється науковцями як метод вивчення правових систем різних держав шляхом зіставлення однойменних правових норм, інститутів, принципів тощо та практики їх застосування [65, с. 157]. Також порівняльно-правовий метод визначають як «сукупність прийомів виявлення загальних і специфічних закономірностей виникнення, розвитку, функціонування правових систем (їх елементів) за допомогою їх порівняння, тобто здійснення пізнавальної операції, що дає змогу на основі фіксованої ознаки встановити подібність або відмінність об'єктів у результаті парного співставлення» [54, с.13]. Тобто порівняльно-правовий метод є нічим іншим як застосування загальнонаукового порівняльного методу до правових явищ. У навчальних джерелах не даремно зазначається, що «для юридичної науки використання порівняльного правознавства є особливо важливим. Відомо, що істина пізнається в порівнянні. Тому без порівняння неможливе з'ясування сутності

будь-якого юридичного феномену. Порівняльне правознавство допомагає встановити, як вирішується та сама правова проблема в різних країнах, і, таким чином, сприяє вивченню національного права. Порівняльно-правовий аналіз здатний озброїти науковця ідеями та аргументами, які не можна отримати при знанні лише національного права. У наш час без врахування даних компаративістики загальнотеоретичні висновки не можуть претендувати на універсальний статус. У межах порівняльного правознавства аналізується й більшість проблем галузевих юридичних наук» [55, с. 20-21]. Тому в юридичній літературі правильно підкреслюється, що використання порівняльно-правового методу є необхідним під час вивчення світового досвіду, пізнання правових явищ у контексті наявних концепцій праворозуміння. На сучасному етапі вітчизняного розвитку в ході проведення правових реформ метод особливо актуальний [10, с. 105]. Підкреслює таку актуальність і Т.С. Подорожна, правильно наголошуючи на важливості порівняльно-правових досліджень з огляду на наявні євроінтеграційні процеси та прагнення нашої держави до вступу в Європейський Союз [53, с. 109].

При цьому вивчення іноземного досвіду правового регулювання використання електронних доказів у процесі судового доказування є цінним як сам по собі, так і в зіставленні з вітчизняними напрацюваннями в даному напрямку, оскільки це допомагає відшукати оптимальний юридичний механізм, який дозволить найбільш ефективно використовувати електронні докази в цивільному судочинстві. Тому є цілком справедливим твердження О. Д. Тихомирова, що «вивчення зарубіжного права, яким воно є «саме по собі», спрямоване на виявлення одиничного, в якому існують загальне, особливе й одиничне, або, іншими словами, непряме використання порівняльного методу. Більше того, в самому терміні «іноземне» чи «зарубіжне» міститься дуалізм одного й іншого, передбачається існування й зіставлення вітчизняного й іншого вітчизняного» [61, с.10].

Домінуючим у порівняльно-правовому методі є прийом порівняння, що дає змогу завдяки зіставленню правових явищ виявляти загальні (спільні), подібні ознаки, на підставі яких здійснюється групування та ідентифікація, а також відмінні, які дають змогу вирізнити утворену групу серед інших [3, с.157-158]. Даний прийом було використано під час вивчення практично кожного кола питань, що досліджувалися під час роботи над дисертацією. Адже зіставлення джерел правового регулювання, принципів, правових інститутів, прямо чи побічно пов'язаних із використанням електронних доказів у процесі судового доказування в цивільному судочинстві країн загального та континентального права було одним із ключових завдань цієї роботи.

Дослідники стверджують, що порівняльно-правовий метод може використовуватись двома способами. Перший спосіб передбачає дослідження обумовленості відповідних правових систем зовнішніми, суспільними чинниками, тоді як другий спосіб ґрунтується на встановленні й порівнянні змісту та складу норм, які є елементами порівнюваних правових систем [53, с.86-87]. У даному дослідженні, в основному застосовувався саме другий спосіб, хоча окремі елементи першого способу також присутні та стосуються, переважно, аналізу впливу нормативних документів Європейського Союзу та Ради Європи на процесуальне законодавство європейських країн.

Варто цілковито підтримати позицію тих науковців, які наголошують на ефективності використання порівняльно-правового методу в правових дослідженнях у сукупності з методами системного аналізу та синтезу, що дає змогу виявити витоки правових явищ, а також наявних нагальних проблем. У цьому контексті важливим є те, що подолання різноманітних проблем, які виникають у процесі реалізації норм конституційного права, досить часто відбувається за допомогою власне компаративістських досліджень, оскільки аналіз вітчизняного чи зарубіжного досвіду дає змогу зробити висновки про можливі шляхи подолання наявних проблем [65, с.157-158]. Також можна цілковито погодитись з А.Ю. Івановою в тому, що застосування

порівняльного методу до систем права різних держав, а, зрештою, до їх позитивного права, є одним з можливих шляхів для пошуку ідеального права, що є центральним завданням права природного [26, с.176].

Дана дисертаційна робота також містить елементи історико-правового порівняльного дослідження. Комбінація порівняльно-історичного та порівняльно-правового методів обумовлюють і комбінацію відповідних ключових підходів. Саме тому основними напрямками реалізації головного завдання в теорії історико-правового порівняльного методу будуть три – історичний, правовий і порівняльний [63, с.181].

Історичний підхід проявляється у спрямованості наукового пізнання із сучасності в минуле, що обумовлює його ретроспективний характер. Крім того, історичне пізнання є опосередкованим внаслідок віддаленості дослідника від історичного об'єкта або явища, що вивчається, а тому позбавляє його безпосереднього контакту з фактами минулого. Звичайно, ретроспективність історичного підходу висуває особливі вимоги до роботи з історичними джерелами, які стають не лише засобами пізнання, але і його об'єктами.

Правовий підхід обумовлений, перш за все, нормативністю права, яка обумовлює існування права як системи юридичних норм, що офіційно визнаються державою та формально визначені, тобто існують у певному матеріалістичному вигляді. Саме нормативність права в порівняльно-правовому дослідженні вимагає від дослідника вміння за допомогою формально-логічних, граматичних та інших засобів тлумачити норми права та правильно розуміти їх.

Сутністю порівняльного підходу в історико-правовому порівняльному дослідженні є співставлення між собою двох або більше порівнюваних об'єктів за певними критеріями з метою отримання інформації про їх подібність або ступінь їх схожості чи відмінності. В основі порівняльного підходу лежить логічна операція порівняння [63, с.181-182].

Наведені підходи використовувалися, зокрема, в процесі дослідження електронних документів у системі судових доказів у цивільному судочинстві Французької Республіки.

Використання порівняльно-правового методу дослідження, окрім іншого, забезпечує тісний взаємозв'язок юридичної науки й практики, адже науковці стверджують, що «порівняльно-правовий метод головним чином сприяє накопиченню емпіричних знань. Теоретичні знання здобуваються завдяки іншим науковим методам. Порівняльно-правовий метод є багатофункціональним, оскільки застосовується і на теоретичному, і на емпіричному рівнях пізнання; до того ж характерним для нього є оціночний підхід. Саме оцінка є суттєвим і необхідним елементом будь-якого порівняння» [49, с.21].

У контексті вищезазначеного, варто погодитись із висловленою в навчально-методичній літературі позицією про те, що правильність («істинність») наукового знання визначається не тільки логікою, але насамперед обов'язковою перевіркою його на практиці. Наукові знання принципово відрізняються від сліпої віри, від беззаперечного визнання правдивим того або іншого положення, без якого-небудь логічного його обґрунтування й практичної перевірки [6, с.14]. Юридична наука не є в цьому сенсі винятком. Звичайно, деякі правники, як і представники інших гуманітарних наук більшою мірою концентруються на формулюванні правових суджень, теоретичних позицій шляхом осмислення, здійснення логічного аналізу досліджуваної проблеми, не завжди спираючись на конкретні емпіричні дані. Однак такий підхід має бути виправданий специфікою предмета наукового дослідження. Емпіричною основою досліджень у сфері цивільного процесуального права є, переважно, матеріали судової практики, ретельне вивчення яких дозволяє наблизити висновки науковця до реалій судової практики та зробити наукове знання не відірваним від реального життя, а, навпаки, таким, що можна практично

застосувати, корисним у повсякденній роботі правників, оскільки сприяє вдосконаленню юридичної практики.

Розвиток юридичної науки передбачає її зв'язок і взаємодію з іншими науками. Як вказує М. Кравчук, «засвоєння та використання знань інших наук відбувається шляхом так званої юридизації методів різних наук і формування нових юридичних дисциплін на межі юриспруденції та суміжних наук» [32, с.116]. Деякі науковці вказують на поєднання у праві методів науки і мистецтва [30, с.28]. Однак в межах даного дослідження більш доцільним та дієвим видається поєднання методів юриспруденції та технічних наук, використання знань про різні інформаційні технології та методи роботи із ними. Вивчення та аналіз різних підходів до правового регулювання використання електронних доказів у процесі судового доказування неможливе без глибокого розуміння технічної основи їх функціонування, розбору різноманітних способів передачі даних, знання наявних інформаційних технологій, особливостей зберігання даних на різних носіях, ризиків, пов'язаних із поширенням електронних даних, можливістю їх копіювання, зміни, видалення та способів відновлення. Тобто процес збирання, дослідження та оцінки електронних доказів потребує від учасників цього процесу доволі суттєвих знань у сфері інформаційних технологій, що не можна не враховувати під час наукових досліджень у цій царині.

Підсумовуючи огляд методів наукового дослідження, варто відзначити, що особливість предмета та обраних методів наукового дослідження зумовили спрямування цієї роботи не лише на розгляд та вивчення принципів, правових норм, інститутів та судових процедур, пов'язаних зі збиранням, дослідженням та оцінкою електронних доказів у процесі розгляду та вирішення цивільних справ, а й відшукування оптимальних засобів правового регулювання використання електронних доказів у процесі судового доказування з метою вдосконалення вітчизняного цивільного процесуального законодавства та судової практики. Тому дослідження було сконцентроване на тих країнах, які вважаються розвиненими як в плані

шанобливого ставлення до демократичних цінностей, захисту прав людини та утвердження справедливого судочинства, так і в плані розвитку інформаційних технологій, а отже вони мають той цінний досвід використання інформаційних технологій у судовому процесі, який може бути вивчений та запозичений Україною.

1.2. Вплив глобалізації та науково-технічного прогресу на формування системи джерел електронних доказів

Жодна правова система, навіть дуже розвинена й самодостатня не може в сучасних умовах існувати цілком відокремлено та самостійно, не піддаючись впливу правових поглядів, інститутів та процедур із інших країн. Як відзначають окремі дослідники, «нині процес єднання людства долає вже не лише національні й регіональні межі, а вийшов на світову арену і відображається вже у глобалізації світового розвитку. Оскільки природні тенденції до єдності людства реалізуються не лише безпосередньо, але й через процес виробництва, обміну, інформацію, духовні зв'язки між народами, то саме промислова цивілізація із значним зростанням виробництва значно посилила цей процес. У цілому тенденція до єдності людства має прогресивний характер і відображається в посиленні зв'язків між представниками різних націй і народностей, в інтернаціоналізації виробництва й обміну, у використанні досвіду побудови політичних структур, у зростанні інформації, обміні духовними цінностями, появі наднаціональних і наддержавних структур та ін.» [2, с.37]. Науково-технічний прогрес лише посилює ці тенденції, оскільки полегшує спілкування та обмін інформацією.

Сучасний науково-технічний прогрес стрімко рухається в бік розвитку інформаційних технологій, які тепер відіграють важливу роль і в цивільному судочинстві. Цілком справедливим є твердження С. А. Чванкіна про те, що

«ІТ надають неймовірні можливості. Миттєвий обмін повідомленнями, можливість купувати, замовляти та отримувати різні блага, інформацію онлайн, – це далеко не повний перелік нових можливостей. Але нові можливості – це і нові ризики, які особливо негативно впливають на сферу надання державних послуг, однією з яких у широкому сенсі й є послуга судочинства. Електронні уряди та електронні суди – запит часу. Соціально-економічний розвиток в епоху цифрових технологій вимагає від держави їх активного використання з метою задоволення швидко мінливих вимог суспільства» [62, с.103].

Різні пристрої здатні створювати та зберігати дані в цифровій формі й такі дані можуть служити доказами. Для початку потрібно ознайомитися з технологіями, їх основними принципами та загальними характеристиками, які відрізняють докази в цифровій формі від будь-яких аналогових доказів у фізичній формі. Зміст цього підрозділу полягає в тому, щоб надати широке ознайомлення з відповідними технічними проблемами, породжені невпинним розвитком інформаційних технологій та висвітлити особливості, які мають бути враховані фахівцем із цифрових доказів і юристом під час дослідження електронних доказів і вирішення проблем із електронними доказами.

Взагалі історично термін «комп'ютер» часто використовувався для опису майже будь-якої форми процесора. Зараз цифрові обчислення та засоби зберігання характерні для багатьох пристроїв, які за формою та функціями здаються далекими від традиційних комп'ютерів. До таких пристроїв належать ігрові консолі, переносні технології (наприклад, фітнес-трекери, розумні годинники) і «розумні» побутові компоненти (наприклад, розумні лічильники електроенергії, автоматизовані системи центрального опалення). Більшість із цих цифрових пристроїв мають спільні важливі функції з більш впізнаваними звичайними комп'ютерними пристроями, такими як настільні комп'ютери, ноутбуки та планшети. Усі ці функції базуються на тому, що іноді називають моделлю вводу-обробки-виводу:

- пристрій отримує певний вхідний сигнал за допомогою локального файлу, датчика, миші, клавіатури або через канал зв'язку (наприклад, підключення до мережі);
- він обробляє інформацію;
- він виводить, наприклад, на дисплей, локальний файл або принтер;
- він повинен мати можливість зберігати (і/або ретранслювати) інформацію;
- він повинен мати можливість контролювати те, що він робить.

Так званий центральний процесор (CPU) є функціональною основною складовою кожного такого пристрою, і сам складається з ряду складових частин. Разом ці частини отримують дані, виконують логічні або арифметичні операції та виводять результати. Результати передаються до локального сховища чи дисплею, або передаються через мережеве з'єднання на інший пристрій [17]. Програмне забезпечення складається з програм, які дають інструкції цифровому пристрою. Існує два основні категорії програмного забезпечення: системне програмне забезпечення та прикладне програмне забезпечення. Системне програмне забезпечення, як впливає з назви, для базової роботи пристрою потрібне системне забезпечення. Набір програм, які керують базовою роботою комп'ютера, називається операційною системою. Операційна система контролює потік даних, розподіляє пам'ять і керує будь-якими апаратними компонентами пристрою, такими як дисплей, пристрій (пристрої) введення, взаємодія з мережею тощо. Операційна система також дозволяє користувачеві керувати будь-якими спеціальними для користувача файлами, що дозволяє кільком користувачам спільно використовувати комп'ютер і діє як інтерфейс між апаратним забезпеченням і програмним забезпеченням [219].

Загалом кажучи, для більш традиційних обчислювальних пристроїв, таких як настільні комп'ютери, ноутбуки та планшети, прикладне програмне забезпечення забезпечує сторону системи, що спрямована на користувача. Це програмне забезпечення «спеціального призначення», яке дозволяє

користувачеві виконувати певні види завдань на комп'ютері. До них належать обробка текстів, настільна публікація, веб-перегляд, електронна пошта, соціальні мережі, підготовка та проведення презентацій, виконання складних наборів числових обчислень тощо. Прикладами прикладного програмного забезпечення є Microsoft Word, Internet Explorer, Outlook, PowerPoint, Excel і LibreOffice. Ці та інші прикладні програми представляють основні причини, з яких більшість людей використовують комп'ютери (тобто для виконання певних завдань, спрощених за допомогою комп'ютера та його прикладного програмного забезпечення). Для інших цифрових пристроїв користувач може використовувати прикладне програмне забезпечення лише за допомогою обмеженого діапазону функцій, таких як перевірка стану на фітнес-трекері або споживання енергії за допомогою інтелектуального лічильника [190].

Ще один компонент, який слід обговорити стосовно роботи цифрових пристроїв: годинник. Годинник виконує дві функції:

1) це пристрій, який створює імпульси часу, щоб гарантувати, що події синхронізовані та відбуваються в передбачуваному порядку. Годинник координує всі компоненти центрального процесора. Кожен крок будь-якої операції має виконуватися в певній послідовності, а деякі операції виконуються з різною швидкістю. Робота системи синхронізується з імпульсами електронного годинника. Частота імпульсів контролюється фазовою автопідстройкою частоти (PLL), яка, у свою чергу, регулюється кристалом кварцу. Швидкість, з якою коливається кристал, коефіцієнт підвищення PLL і кількість кроків, які вимагає кожна інструкція, визначатимуть швидкість, з якою працює комп'ютер;

2) годинник також часто служить для визначення часу доби та дати в людському розумінні. Більші комп'ютерні системи синхронізують свої годинники з надійним джерелом часу, доступним через інтернет, за допомогою системного інтерфейсу, такого як мережевий протокол часу. Це дозволяє пристроям, підключеним до інтернету, синхронізувати

налаштування часу (з урахуванням географічного положення та часових поясів).

Є дві важливі причини для забезпечення синхронізації часу. Перша мета полягає в тому, щоб події відбувалися вчасно та в правильній послідовності, що дозволяє планувати події та точно реєструвати факт, що вони відбулися. Друга мета полягає в тому, щоб дати людині можливість отримати інформацію про минулі події, включаючи встановлення часу та послідовності, в якій вони відбулися. Це можливо лише за наявності точних позначок часу. Наприклад, механізм позначення часу для автентифікації, цифрових підписів, відправлення листа, діагностики несправностей, записаних у системних журналах подій і т.д.

Також слід зазначити, що годинник у цифрових пристроях часто неточний (як недорогий наручний годинник), що ускладнює дослідження фактів як доказів. Зазвичай годинник можна налаштувати (і навіть неправильно встановити) вручну. Це може призвести до того, що системний годинник буде дещо неправильним (через «дрейф у відліку часу») відносно фактичного часу в локальному регіоні. Така неточність може вплинути на обидва способи використання годинника, зазначені вище, тобто на планування подій і їх запис, оскільки обидва аспекти можуть залежати від часу, отриманого від системного годинника. Там, де важлива точність часу, годинник зазвичай потребує час від часу коригування, щоб привести час у відповідність із кращими довідковими джерелами (наприклад, серверами часу в інтернеті). Це питання має певне значення, оскільки безсумнівні та вирвані з контексту припущення щодо точності чи неточності годинника можуть призвести до оманливого висновку.

З точки зору електронних доказів, системний годинник часто відіграє життєво важливу роль у відмітці часу. Наприклад, операційна система використовує налаштування дати й часу, щоб нотувати свій запис подій, таких як створення або зміна файлу. У комп'ютерах таку інформацію часто називають «метаданими» файлу (дані, які описують або інтерпретують базові

дані), оскільки інформація про дату й час пов'язана з файлом, але не є частиною даних у файлі чи даних над якими користувач має будь-який прямий контроль. Позначки часу також записуються для системних подій, таких як вхід користувачів, відкриття електронного листа, зміна пароля, і, залежно від призначення пристрою, події, зареєстровані датчиками, наприклад такі, як кількість кроків, пройдених користувачем. Інформація про час і дату, пов'язана з такими подіями, записується у файли системного журналу (журнали подій). Такі журнали часто є важливим джерелом інформації про послідовність подій і дають змогу зрозуміти передбачувану конкретну діяльність користувача, що служить підтвердженням чи спростуванням факту, що досліджується.

Як зазначалося раніше, годинник на комп'ютері може встановлювати користувач і може бути налаштований для підтримки неправильного поточного часу (наприклад, за допомогою мережевого протоколу часу). Неправильні налаштування часу будуть відображені в мітках дати й часу, згодом записаних системою. Очевидно, що цю потенційну аномалію слід враховувати, коли маємо справу з даними з часових міток. Оскільки часовий пояс також встановлюється в системі, неправильний вибір поясів може призвести до неправильної поточної дати або часу. Крім того, через важливу роль, яку відіграє годинник, він містить велику кількість електронних доказів, особливо там, де ним маніпулює відповідач, щоб приховати докази змін, внесених у важливі докази [33].

Для збереження програм, результатів виведення та інших даних, на основі яких працюють програми, цифрові пристрої покладаються на пам'ять. Загалом існує дві форми зберігання: первинне зберігання та вторинне зберігання. Основне сховище – це сховище, до якого процесор має прямий доступ. Зазвичай він має форму напівпровідникової пам'яті, наприклад:

- мікросхема внутрішньої пам'яті, відома як пам'ять із довільним доступом (RAM). Ця мікросхема здатна багаторазово зберігати (записувати) й отримувати збережені дані (читати).

- мікросхема внутрішнього зберігання, яка здатна зберігати дані один раз, але не дозволяє перезаписувати дані. Після введення даних цей тип чіпа дозволяє лише зчитувати дані. Це називається постійною пам'яттю (ROM) [47].

- мікросхема внутрішньої пам'яті, яка зберігає дані та веде себе як ПЗП під час нормальної роботи, але дозволяє видаляти та замінювати дані. Ця форма пристрою відома як програмована постійна пам'ять, що стирається, (EPROM). Флеш-ПЗП є різновидом EPROM [121].

Вторинна пам'ять – це пам'ять, до якої процесор не має прямого доступу. Якщо потрібні дані, на яких вони зберігаються, процесор використовуватиме свої канали введення/виведення, щоб отримати доступ до вторинного сховища та перенести необхідні дані в основне сховище. На відміну від основного сховища, вторинне сховище є енергонезалежним: воно зберігає свої дані, коли пристрій вимкнено. Жорсткі диски (HDD) і USB-накопичувачі як носії інформації є типовими формами вторинного зберігання. Вони можуть бути постійно під'єднані до комп'ютера (внутрішня пам'ять) або підключені за потреби (зовнішня пам'ять). Інші форми зовнішнього сховища можуть бути менш близькими до комп'ютера, наприклад, мережеве сховище (NAS) [35], різні накопичувачі або «хмарне» сховище.

Оскільки вторинне сховище є енергонезалежним, жорсткий диск і пов'язані з ним автономні носії є важливим джерелом електронних доказів для пристрою. Але той факт, що пам'ять є енергонезалежною, не означає, що її дані не можна отримати після видалення. Експеримент із «заморожуванням» мікросхем оперативної пам'яті перед фізичним видаленням і перенесенням на інший комп'ютер виявив незвичний контекст, у якому дані оперативної пам'яті можуть бути відновлені з оброблених мікросхем [13].

Дедалі більша різноманітність способів зберігання цифрових даних і різноманіття контекстів зберігання означає, що пошук відповідних даних як

потенційних доказів може бути непростю справою. Дані можуть зберігатися локально на комп'ютерному пристрої, наприклад на жорстких дисках, DVD або компакт-дисках, флеш-накопичувачах, картах пам'яті або мікропристроях пам'яті (які зазвичай зустрічаються у смартфонах). Але дані також можуть зберігатися віддалено, наприклад, у мережевому сховищі, у віддалених мережах або «хмарних» об'єктах. Багатьох цифрових експертів хвилюють труднощі, пов'язані з визначенням місцезнаходження та отриманням легального доступу до даних, які зберігаються віддалено з комп'ютера особи.

Експерт із цифрових доказів може виявити ряд «втрачених даних на жорсткому диску чи іншому носії інформації в декількох випадках:

- якщо користувач навмисно позначає частини жорсткого диска як «погані», він може приховати значні обсяги даних у цих частинах, які неможливо побачити без використання відповідного засобу діагностики або перевірки диска (оскільки операційна система буде автоматично уникати будь-якого використання цих «пошкоджених секторів»);

- коли користувач видаляє дані, вони залишаються на диску, доки старий файл не буде перезаписано новими даними. Видаляються лише покажчики системи в системі файлів. Навіть якщо частину файлу було перезаписано, часто можна відновити частину видаленого файлу, якщо весь набір дискових блоків, що містять вихідний файл, не було повністю перезаписано.

Однак із цього не випливає, що відновлені дані є справжніми чи надійними доказами лише тому, що їх знайдено. Є багато ситуацій, у яких дані можуть бути втрачені або пошкоджені, і це вплине на достовірність будь-яких відновлених даних. Приклади включають пошкодження або втрату даних через помилки в програмі та втручання в дані із зовнішніх джерел [51]. Крім того, слід зауважити, що на надійність доказів також вплине спосіб, у який експерт із цифрових доказів проводить перевірку та відновлює дані.

Взагалі, електронні докази можуть бути широко класифіковані на цифрові дані, де інформація представлена в двійковій формі, і текстові дані, включаючи дані з буквами, цифрами та знаками пунктуації. Текст можна ввести в комп'ютер кількома способами:

1) Введення літер, цифр і знаків пунктуації, головним чином за допомогою клавіатури.

2) Сканування сторінки за допомогою сканера зображень і перетворення зображення в дані за допомогою програмного забезпечення оптичного розпізнавання символів (OCR) [48].

3) Використання штрих-коду. Штрих-код представляє буквено-цифрові дані. Штрих-код зчитується за допомогою оптичного пристрою, який називається паличкою. Відсканований код перетворюється на двійкові сигнали, що дозволяє компоненту трансляції штрих-коду зчитувати дані.

4) Зчитування магнітної смуги на звороті кредитної картки.

5) Голосові дані, коли людина говорить у мікрофон, здатний записувати звуки. Ця форма даних, як і відеодані, кодується у двійковій формі.

6) Перетворення мови в текст. У цьому випадку користувач говорить у мікрофон, підключений до комп'ютера, а спеціальне програмне забезпечення аналізує вхідний сигнал і перетворює його на текстове представлення вимовлених слів.

Щоб дозволити користувачеві переглядати текст і числа, а також бачити зображення чи чути звук, двійкова форма даних має бути перетворена за допомогою коду. Двійкову інформацію можна представити за допомогою двійкової (основа 2) системи числення, хоча більш поширеним є представлення комп'ютерних чисел у вісімковій (основа 8) або, найчастіше, шістнадцятковій (основа 16).

Для текстових даних існує ряд кодів. Деякі коди, які широко використовуються, відомі як Юнікод [162], Американський стандартний код для обміну інформацією (ASCII) [225], Розширений двійковий код

десятьового обміну кодами (EBCDIC) [232] і Формат перетворення Юнікоду-8 (UTF-8) [233] - це стандартний код символів, який використовується в Інтернеті й здатний кодувати всі можливі символи. Зараз більшість комп'ютерів використовують Unicode та ASCII. Доступні інструменти для відображення двійкових даних, які використовуються в комп'ютерах, щоб цифровий дослідник міг переглядати функції, які зазвичай не бачать користувачі комп'ютера. Наприклад, документи, збережені у форматі Microsoft Word, містять метадані програми, які зазвичай невидимі. Використовуючи певні типи програм, дослідник електронних доказів може переглядати всі аспекти даних, і такі дані можуть виявити важливу інформацію, яка може допомогти доказуванню.

Щоразу, коли електронний пристрій увімкнено, різні компоненти повинні взаємодіяти один з одним, щоб він почав працювати. Це називається процесом запуску або «завантаженням» системи. Більшість пристроїв мають програму в пам'яті лише для читання, яку по-іншому називають завантажувачем, процесом завантаження, завантажувальним ремнем або початковим завантаженням програми. У загальних рисах це працює так:

- коли систему ввімкнено, керування спочатку передається базовій системі введення та виведення (BIOS) [83], програмі, яка постійно знаходиться в ПЗП пристрою;

- BIOS перевіряє різні компоненти системи, перевіряючи їх активність і працездатність. Результати різних тестів, які він виконує, можуть відобразитися на виході системи. Процес завантаження також може очистити локальну первинну пам'ять від усіх історичних даних і метаданих. BIOS знаходить перший (або за замовчуванням) вторинний запам'ятовуючий пристрій, шукає операційну систему на запам'ятовуючому пристрої та передає керування запису завантаження операційній системі (набір інструкцій, що починаються з певного місця на запам'ятовуючому пристрої);

- завантажувальний запис бере на себе контроль над системою. Ця програма також містить завантажувач, який, у свою чергу, завантажує та перевіряє конфігурацію перед завантаженням операційної системи;

- нарешті, операційна система відобразить будь-яке діалогове вікно запуску (наприклад, ідентифікатор постачальника послуг мобільного зв'язку) і, якщо користувач авторизований (наприклад, шляхом введення коду), надасть доступ до програм прикладного рівня і користувач може керувати пристроєм через додаток.

Експерт із електронних доказів може зробити низку доказів доступними з електронного пристрою. Далі наведено опис деяких типів доказів, які можна зібрати і використовувати як докази в суді.

Широкий спектр прикладного програмного забезпечення, що використовується на комп'ютерах, ноутбуках, планшетах і мобільних телефонах, включаючи програми, дозволяють користувачеві надсилати повідомлення, готувати електронні таблиці, бази даних і текстові документи, робити цифрові фотографії та створювати мультимедіа та презентації. Файли, в яких зберігатимуться повідомлення, електронні таблиці, бази даних, тексти, фотографії, мультимедіа та презентації самі по собі можуть бути електронними доказами. Можна отримати велику кількість даних залежно від методу зберігання, передачі і способу, яким пристрій керує зберіганням даних.

Будь-яка судова експертиза розпочнеться зі створення копії зображення пристрою, на якому можуть зберігатися електронні докази. Процес створення зображень – це неруйнівний процес, який створює точну зовнішню цифрову копію будь-яких даних на пристрої. Згодом усі дослідження даних слід виконувати на копії зображення, а не на даних, що зберігаються на оригінальному пристрої.

У більшості сучасних операційних систем, таких як Windows і Linux, практично все, що відбувається в системі та з нею, певним чином записується у вигляді журналів. Це включає інформацію про системні події, включаючи

запуск програм і різні класи повідомлень про помилки. Інформація в журналах може допомогти визначити, наприклад, як неавторизований користувач комп'ютера отримав доступ до системи з наміром викрасти інформацію з комп'ютера. Також можливо налаштувати системний журнал (syslog), щоб повідомлення журналу могли надсилатися в іншу мережеву систему, зберігаючи локальну копію. У результаті, якщо хакер отримує привілеї root у мережевій системі UNIX, наприклад, і хоче стерти щось із локальних журналів, він не зможе стерти дані з віддалених журналів, щоб видалити всі сліди свого вторгнення.

На відміну від систем UNIX, операційна система Windows також містить «реєстр». Це сховище даних, яке містить велику кількість інформації, включаючи повну базу даних, що містить інформацію про кожну програму, сумісну з Windows, встановлену на комп'ютері. Він також містить інформацію про передбачуваного користувача комп'ютера, переваги, які використовує користувач, інформацію про апаратні компоненти та інформацію про мережу (якщо її підключено до мережі). Значення, що зберігаються в реєстрі, мають шістнадцятковий формат, але їх можна конвертувати в ASCII. Прикладом типу інформації, яку сторона може надати суду є дані автозаповнення для користувача Internet Explorer, який відвідує певний вебсайт, наприклад його ім'я, адреса, номер телефону, адреса електронної пошти та паролі. Крім того, з реєстру можна встановити, коли користувач востаннє завантажував файл з інтернету, а також першу сторінку, яку відвідав користувач [210].

Коли комп'ютер під'єднується до інтернету, деяка інформація про його діяльність записується та зберігається локально, включаючи відвідані вебсайти, вміст, який переглядався, і будь-які відвідані групи новин. Щоб покращити роботу браузера та прискорити перегляд, тимчасові копії відвіданих вебсайтів зберігаються в кеш-папках. Ці папки містять фрагменти вебсторінки, включаючи зображення та текст. Деякі версії програмного

забезпечення зберігають у кількох локальних файлах інформацію про відвідані вебсайти.

Крім кешу браузера, системи Windows і UNIX також мають файл підкачки або простір підкачки. Це область диска, яка використовується як віртуальна пам'ять. У випадку, якщо програми, які працюють у системі, вимагають більше оперативної пам'яті, ніж доступна системі, запущені програми з низьким пріоритетом копіюються у віртуальну пам'ять, а оперативна пам'ять, яку вони використовують, звільняється для використання програмами з вищим пріоритетом. Під час нормальної роботи системи простір підкачки рідко очищається. Це означає, що коли потрібно проаналізувати систему для судової експертизи, корисні дані, пов'язані з програмами, які на той момент можуть бути навіть не запущені, часто можна знайти шляхом аналізу вмісту простору підкачки. Це також може стосуватися даних, які зазвичай зберігаються в стандартній файловій системі в зашифрованому вигляді. Залежно від програми та конкретних обставин деякі програми можуть дозволяти зберігати незашифровані копії даних у файлі підкачки.

Файлові системи зберігають записи про розташування даних на носії інформації. Спосіб зберігання даних буде відрізнятися залежно від програмного забезпечення та побудови методу, який використовується для виділення блоків зберігання для файлів. Простіше кажучи, розташування даних на носії інформації контролюється файловою системою. Наприклад, носій даних можна розділити на розділи, і в цьому випадку файл зберігатиметься в певному місці розділу. Коли файл видаляється, вказівка на видалення видаляє вказівник на розташування файлу, але фактично не видаляє файл. З цієї причини в переважній більшості випадків можливо відновити видалені дані залежно від обсягу запису на диск, який було виконано між видаленням файлу та судовою експертизою [98]. Крім того, якщо пристрій, який, як стверджується, не функціонує, було відновлено або розблоковано судовою експертизою, то можна виявити чи зробити висновок

про порушення на пристрої. Це ілюструє справа Sectrack NV проти Satamatics Ltd щодо неправомірного використання конфіденційної інформації. В одного зі сторін був пристрій Blackberry, який, як він стверджував, був заморожений або заблокований. Коли пристрій було «розблоковано», він автоматично завантажував різні електронні листи, які отримувач відповідач, що вказувало на його причетність до зловживання конфіденційною інформацією. Після цієї справи виробники портативних пристроїв розробили широкі системи резервного копіювання, які дозволяють передачу даних пристрою на інші пристрої та засоби зберігання. У майбутньому без використання шифрування буде відносно важко видалити дані настільки, щоб їх неможливо було відновити.

Портативні пристрої тепер поширені всюди. До них відноситься використання планшетів і смартфонів, які поєднують функціональність персонального комп'ютера з телефоном і камерою. Такі пристрої є комп'ютерами, оскільки вони мають центральний процесор, пам'ять, клавіатуру (вхід) і екран або динамік (вихід). Як і комп'ютери, портативні пристрої мають ПЗП та ОЗП. ПЗП зберігає операційну систему та будь-яке важливе програмне забезпечення, необхідне для роботи пристрою. Оперативна пам'ять використовується для зберігання іншого програмного забезпечення та даних, які користувач може захотіти зберегти. Зовсім недавно ці пристрої стали оснащуватися програмованим ПЗП, відомим як flash-ROM, різновидом твердотільного чіпа пам'яті, який здатний зберігати вміст без живлення.

Інші типи спеціалізованих мобільних пристроїв включають цифрові музичні програвачі та пристрої для читання електронних книг, які можуть використовувати бездротову технологію для завантаження великих обсягів даних із основного комп'ютера. Усі ці пристрої разом із портативними комп'ютерами все частіше використовуються організаціями як компоненти розширеної інфраструктури інформаційних технологій. У відповідних випадках такі пристрої можуть бути досліджені на наявність електронних

доказів, хоча обсяг інформації, яку можна отримати, буде різним. Наприклад, хоча можна знайти лише список останніх телефонних номерів, на які телефонували зі звичайного мобільного телефону, смартфон, ймовірно, видасть значні обсяги даних, включаючи електронні листи та інші дані з мережі, які можуть допомогти про розгляді справи в суді.

Наведені вище приклади підкреслюють типи електронних доказів, які можуть бути виявлені за допомогою судової експертизи, включаючи приховані або видалені дані. Лише висококваліфікована людина може видалити всі сліди доказів на комп'ютері, а такі навички дуже рідкісні. Існують деякі методи, які можуть відновити дані, навіть якщо вони були повністю перезаписані на диску. Чи будуть ці методи використовуватися, звичайно, залежатиме від типу та цінності даних, які потрібно відновити.

Пройшли ті часи, коли більшість комп'ютерів стояли окремо на столі. Зараз більшість комп'ютерів під'єднані або періодично під'єднані до інших комп'ютерів чи мережі. Враховуючи сліди, залишені різноманітними журналами та файлами в комп'ютерах, вихід в Інтернет може створити велику кількість електронних доказів, включаючи використання електронної пошти, підключення до Інтернету та перегляд веб-сайтів, а також передачу файлів між комп'ютерами. Інші джерела електронних доказів можна отримати з серверних журналів, вмісту пристроїв, підключених до мережі, і записів трафіку. У багатьох випадках може статися так, що єдиний доказ, який буде доступний, — це доказ у мережі, оскільки сторона могла успішно переконати іншу сторону знищити докази, позбувшись свого жорсткого диска та будь-якого іншого обладнання.

З появою Всесвітньої павутини людям стало легше користуватися Інтернетом. Існують також інші мережі, які працюють на вищих швидкостях, наприклад Інтернет-2. Коли комп'ютер під'єднується до Інтернету, він використовує набір протоколів під назвою «Протокол керування передачею/Інтернет-протокол» (TCP/IP) [78]. Цей набір стандартів зв'язку можна розглядати як загальну мову, яка дозволяє спілкуватися між різними

типами мереж, з іншим. Коли комп'ютер під'єднано до мережі, його називають «хостом». Комп'ютер використовує модем або плату мережевого інтерфейсу (NIC) [31] для надсилання та отримання інформації, хоча середні та великі організації мають шлюз локальної мережі (LAN) [34] до інтернету. Комп'ютер або хост, під'єднаний до двох чи більше мереж, називається «маршрутизатором», якщо він є посередником у проходженні трафіку між ними та якщо мережі мають різні адреси. Більшість мереж використовують індивідуальні маршрутизатори. Маршрутизатори є дуже важливою частиною мережі, оскільки вони спрямовують дані з однієї мережі в іншу, фільтрують недозволений трафік і зберігають журнали активності. Більшість маршрутизаторів ведуть системні журнали, які можуть відрізнятися за кількістю даних і кількістю деталей у кожному записі журналу.

Наступним компонентом сучасної комунікаційної інфраструктури є сервер, який часто розглядають як дуже потужний комп'ютер, який надає низці клієнтів послугу, наприклад, розміщення вебслужби організації або засобів електронної пошти. Деякі сервери, наприклад вебсервери, дозволяють будь-кому отримувати доступ до своїх ресурсів без обмежень. Інші сервери, такі як сервери електронної пошти, дозволяють лише авторизованим користувачам отримувати доступ до служби, зазвичай за допомогою імені користувача та пароля. Джерела електронних доказів із серверів включають записи журналів, коли користувач підключається до сервера, незалежно від того, надає він доступ до інтернету чи завантажує електронну пошту.

Інтранет, якою зазвичай керує велика організація, є приватною мережею, яка в принципі доступна лише для членів і співробітників організації або інших осіб, які мають дозвіл на отримання доступу та використання інформації, що міститься в мережі. Інтранет може виглядати як зменшена версія інтернету, що містить вебсайти, поштові сервери та сервери часу серед інших можливостей. Інтранет, який зазвичай розташовується в межах корпоративного захисту, створюється для підтримки внутрішніх потреб організації, а також для покращення зв'язку між робочою силою та

бізнес-операціями. Таким чином, він, зазвичай, спрямований на те, щоб сторонні особи не мали доступу до організації, і зазвичай добре захищений.

Подальшим розвитком цієї форми мереж є бездротова технологія. Однією з реалізацій бездротової мережі є Wi-Fi (марка, що використовується Wi-Fi Alliance [230]), головним чином через радіодіапазони 2,4 ГГц і 5 ГГц на основі стандарту зв'язку 802.11. Інша бездротова технологія, відома як Bluetooth, є стандарт бездротової технології для обміну даними між пристроями на короткій відстані за допомогою радіохвиль ультрависокої частоти (УВЧ) [84]. З точки зору доказів, журнали існують для запису використання бездротових мереж, що є доказом того, як пристрій використовував мережу.

Стільникова мережа або мобільна мережа — це комунікаційна мережа, яка дозволяє портативним пристроям, таким як стільникові телефони, спілкуватися один з одним. Мережа складається з ряду стільникових станцій (базових станцій) у межах певної географічної області. Особа, підключена до стільникового сайту, може здійснювати та приймати дзвінки через мережу. Кожен стільниковий вузол, підключений до центральної обчислювальної інфраструктури, що включає телефонні станції або комутатори, які, у свою чергу, підключені до телефонної мережі загального користування. Ця інфраструктура обробляє дзвінки, направляючи їх до місця призначення, і зберігає журнали з метою надсилання рахунків, обслуговування та, якщо необхідно, проведення експертизи. Найновіші розробки в стільникових технологіях включають послуги загального пакетного радіозв'язку (GPRS), Універсальну мобільну телекомунікаційну систему третього покоління (3G) (UMTS) і стандарт довгострокової еволюції (LTE) четвертого покоління (4G), розробки, які забезпечують більш високі швидкості передачі даних і такі програми, як мобільний доступ до інтернету, IP-телефонія, ігрові послуги, мобільне телебачення високої чіткості та відеоконференції. Вони витісняють стандарт Глобальної системи мобільного зв'язку (GSM), який, хоч і містить

механізми шифрування, зараз вважається таким, що має недоліки безпеки, які складно, хоча й можливо, використовувати [149].

Мобільний телефон має кілька номерів, які ідентифікують пристрій. Виробник включає електронний серійний номер (ESN) [117] або номер International Mobile Equipment Identity (IMEI) [155], як код для унікальної ідентифікації мобільних пристроїв. Номер International Mobile Subscriber Identity (IMSI) [156] — це унікальний ідентифікаційний номер, який зазвичай надається на SIM-карті телефону для ідентифікації абонента стільникової мережі. Щоб запобігти ідентифікації абонента, цей номер надсилається рідко. Замість нього надсилається тимчасовий ідентифікатор мобільного абонента (TMSI) [181], який генерується випадковим чином і призначається телефону в момент його ввімкнення, щоб забезпечити зв'язок між мобільним пристроєм і базовою станцією. Нарешті, ідентифікаційний номер мобільного зв'язку (MIN) або ідентифікаційний номер мобільної підписки (MSIN) [180] - це унікальний номер телефонного довідника для цієї мобільної підписки, який використовується для ідентифікації телефону. Він походить від останньої частини IMSI.

Щоб переконатися, що телефонна компанія знає правильну базову станцію для направлення виклику, місцезнаходження телефону постійно відстежується, коли він увімкнено. Таким чином, існує широкий спектр електронних доказів, пов'язаних із використанням мобільного телефону, включно з географічним розташуванням телефону, деталями здійснених і отриманих дзвінків, а також відновленням вмісту текстових повідомлень. Якщо телефон здатний використовувати й інші способи, наприклад, здійснення мікроплатежів, дані, пов'язані з такими послугами, також можна отримати [214].

Значна кількість листування, що здійснюється всередині та між організаціями, має форму обміну електронною поштою. Електронна пошта — це, по суті, неструктурована форма спілкування, зміст якої визначає її мету:

1) Електронний лист із внутрішнім обговоренням офіційних питань між працівниками є внутрішнім меморандумом.

2) Подібний електронний лист, надісланий третій стороні, пов'язаний із офіційною справою, є зовнішнім зв'язком і, будучи надісланим із тією ж корпоративною інформацією, що міститься на канцелярських товарах, має розглядатися як офіційний канцелярський матеріал.

3) Продовженням телефонної розмови, яке підтверджує щось, наприклад, є примітка, яка буде додана до файлу, незалежно від того, чи надіслано воно людям усередині організації, чи зовнішнім адресатам, чи комбінації внутрішніх і зовнішніх адресатів.

Електронна пошта є важливим джерелом електронних доказів. Однак до електронних листів слід ставитися з деякою обережністю, оскільки людина може відносно легко приховати свою особу та сховатися за фальшивою адресою електронної пошти. Дуже просто надіслати електронний лист, який, здається, надійшов від справжнього джерела. Підrobка електронних листів може бути легкою, але електронна пошта вільно допускається до судових процесів, як кримінальних, так і цивільних.

Щоб отримати доступ до електронної пошти, необхідно взаємодіяти з двома різними службами: однією для вихідної та іншою для вхідної пошти. Ці послуги можуть надаватися або не надаватися одним сервером. Щоб прочитати електронну пошту, особа повинна наказати програмі електронної пошти підключитися до поштового сервера за допомогою одного з кількох протоколів, найпоширенішими з яких є: протокол поштового відділення (POP) [183], протокол доступу до повідомлень інтернету (IMAP) та власний протокол корпорації Майкрософт, який називається інтерфейсом програмування програм обміну повідомленнями (MAPI) [175].

Протокол POP дозволяє користувачеві читати свою електронну пошту, завантажуючи її з віддаленого сервера в сховище свого локального комп'ютера або пристрою. Після завантаження електронного листа з сервера, він автоматично видаляється з активного сервера, але, ймовірно, не з

резервного сервера, який незмінно використовуватиметься постачальником поштових послуг для відновлення після збою з будь-якої причини. Навпаки, протокол IMAP дозволяє користувачеві залишати всю свою електронну пошту на поштовому сервері. Зберігання всієї електронної пошти на одному сервері може бути перевагою для організації, оскільки для електронної пошти всієї організації можна створювати резервні копії з центрального розташування. Однак проблема збереження всіх електронних листів на сервері полягає в тому, що сервер може з часом перевантажитися через обсяг даних. І протоколи POP, і IMAP вимагають від користувача імені користувача та пароля, перш ніж він зможе отримати доступ до служби завантаження пошти. Крім того, сервери протоколу зберігають журнали про те, хто перевіряв електронні листи та коли їх перевіряли. Це дає змогу експерту шукати докази трафіку електронної пошти, навіть якщо користувач видалив усі свої листи.

Вихідна електронна пошта використовує інший протокол під назвою Simple Mail Transfer Protocol (SMTP), хоча MAPI також підтримує вихідну електронну пошту. Сервери, що підтримують SMTP, зазвичай не вимагають від користувача використання пароля. Завдяки цьому людині дуже легко підробити повідомлення. Однак сервер SMTP може вести журнал повідомлень, які проходять через систему [14].

Коли електронний лист надсилається з комп'ютера, він переходить до одного з кількох агентів передачі повідомлень (MTA). MTA діють так само, як поштові відділення. Місцевий MTA отримає електронний лист. Після отримання він додасть до верхньої частини отриманого електронного повідомлення поточний час і дату, назву MTA та іншу додаткову інформацію. Коли повідомлення проходитиме через різні MTA, кожен MTA додаватиме додаткові позначки дати та часу до заголовка. Остання інформація буде у верхній частині заголовка.

Іншим елементом інформації, який зазвичай збирається в заголовку, є адреса інтернет-протоколу (IP) комп'ютера або системи, що підключається

до сервера. Технічно спритні користувачі електронної пошти, які, можливо, бажають приховати свою особу, можуть надсилати повідомлення через анонімні або псевдонімні служби повторної розсилки. Коли електронна пошта надсилається через такий агент повторної розсилки, інформація заголовка може бути видалена, перш ніж повідомлення буде надіслано адресату. Однак деякі інші форми електронних доказів передаються під час такого процесу, і судові експерти можуть спробувати знайти докази, які можуть бути корисними [102].

Обмін миттєвими повідомленнями (IM) — це форма онлайн-комунікаційної служби, яка дозволяє користувачеві передавати різноманітні текстові, голосові та графічні повідомлення іншим особам у режимі реального часу через інтернет. Ця форма спілкування схожа на розмову телефоном, але користувачі зазвичай спілкуються, вводячи повідомлення в програмне забезпечення. Технологія також дозволяє користувачеві обмінюватися файлами. Обмін миттєвими повідомленнями став популярним, оскільки програмне забезпечення, яке реалізує цю послугу, можна завантажити безкоштовно, його легко встановити та використовувати [138].

Залежно від типу програмного забезпечення, яке використовується, програма, коли ініціюється повідомлення, з'єднує два пристрої за допомогою прямої конфігурації «точка-точка» або через конфігурацію клієнт-сервер через порти пристроїв. Є дві суттєві проблеми. По-перше, у конфігурації клієнт-сервер, сервер миттєвих повідомлень може не обов'язково реєструвати такі повідомлення, що означає, що такі розмови можна вважати концептуально подібними до розмов по телефону. По-друге, програма може мати функцію, яка дозволяє повідомленням проходити через законні відкриті порти, якщо інші недоступні. Чи записуватимуться такі розмови, залежить від використовуваного програмного забезпечення. У ранішому варіанті обміну миттєвими повідомленнями, відомому як інтернет-чат (IRC), розмови відбуваються подібно до конференц-дзвінка. IRC в основному призначений для групового спілкування, хоча він також дозволяє спілкуватися сам на сам

через приватні повідомлення. Він часто страждає від тих самих проблем, що й обмін миттєвими повідомленнями, оскільки сервери, які ретранслюють повідомлення, зазвичай не налаштовані для реєстрації розмов [92].

З розвитком персональних комп'ютерів збільшувалася їх місткість і потужність. У результаті між клієнтом і сервером стає менше лінії розмежування. Це пояснюється тим, що будь-який хост можна зробити сервером, встановивши відповідне програмне забезпечення на комп'ютер. Потім програмне забезпечення дозволяє іншим клієнтам отримати доступ до ресурсів комп'ютера через мережу. Це називається одноранговою мережею (P2P) і часто є предметом судових спорів щодо інтелектуальної власності, особливо з метою безкоштовного завантаження музики та фільмів [133]. Наприклад, у Гонконзі було видано наказ Norwich Pharmacal у справі Cinopoly Records Co Ltd проти Hong Kong Broadband Network Ltd щодо низки IP-адрес, а у справі Polydor Ltd проти Брауна було винесено спрощене рішення проти другого відповідача, пана Боулза, за порушення авторських прав після того, як Norwich Pharmacal було винесено судовий наказ проти різних інтернет-провайдерів, чиї IP-адреси абонентів були ідентифіковані як такі, що використовувалися для ймовірно недобросовісної діяльності. В обох випадках порушників було ідентифіковано інтернет-провайдерами на основі їхніх електронних записів IP-адрес, призначених їхнім абонентам у відповідну дату та час, коли мала місце ймовірна недобросовісна діяльність [189].

Поява Web 2.0 призвела до величезного збільшення кількості веб-сайтів, які дозволяють користувачам надавати власний вміст. Це різний тип: завантажені відеокліпи (на таких сайтах, як YouTube), фотографії (на таких сайтах, як Flickr), особисті роздуми у формі блогів (особистих веб-журналів) та інтерактивні обміни з ширшою аудиторією у формі соціальних мереж. Сайти (такі як Facebook і Twitter) та їх більш орієнтовані на бізнес альтернативи (такі як LinkedIn). У міру зростання популярності соціальних мереж із стрімким зростанням кількості користувачів, що беруть участь,

виникає кілька контекстів, у яких вміст соціального внеску особи може бути доказом. Наприклад, особу можна знайти в певному місці за допомогою її повідомлень на такому сайті з геотегами, а фотографії, завантажені на сайт соціальної мережі, часто зберігають свої дані геотегів і відображають час і місце, де вони були зроблені.

З іншого боку, внесок особи в соціальну мережу може бути достатнім для визначення політичних або соціальних упереджень, які, у свою чергу, проливають світло на характер свідка. Докази в таких випадках можуть бути отримані з дописів свідків на сайтах соціальних мереж, залежно від наявності та доступності таких внесків на таких сайтах. Якщо особа зробила такі внески під псевдонімом, фахівець із цифрових доказів може встановити його справжню особу, зіставивши його онлайн-внески з тим самим вмістом, що знаходиться на носіях інформації цієї особи.

Враховуючи всюдисущість електронних пристроїв і нашу майже повну залежність від них, спектр електронних доказів, які можна зафіксувати, дослідити та розкрити в судовому процесі, дуже широкий, як показано в цьому підрозділі. Від файлів на цифровій камері до складної поведінки комп'ютера, підключеного до інтернету, оцінка електронних доказів стала основною частиною життя юриста. Кожен юрист повинен бути готовий надавати відповідні поради своїм клієнтам щодо збирання, розкриття, прийнятності та поводження з такими електронними доказами. Проте в кожній країні своє законодавство щодо того, які електронні докази можуть вважатися належними та допустимими. Усі ці питання будуть належним чином розглянуті в наступних розділах.

Як вбачається з проведеного аналізу, електронні докази за способом вираження інформації поділяються на два види: 1) інформація представлена в двійковій формі; 2) інформація, інтерпретована за допомогою програмного забезпечення у текст, звук, зображення тощо. Вказані способи вираження доказової інформації відрізняються за порядком використання їх в судовому процесі. Якщо інформація першого виду може бути досліджена лише

експертом та залучається в судовий процес опосередковано через висновок експерта, то другий вид інформації може бути досліджений судом безпосередньо.

Підсумовуючи вищезазначене, можна побудувати дворівневу модель системи електронних доказів, залежно від особливостей джерел їх отримання та способу використання у процесі судового доказування: перший рівень - електронні докази, які за характеристиками матеріального носія та електронної інформації можуть бути безпосередньо доставлені в судові засідання та досліджені судом без використання спеціальних знань; другий рівень - електронні докази, які або через особливості носія не можуть бути доставлені до суду, або специфіка електронної інформації, яку вони містять, не дозволяє їх дослідження без застосування спеціальних знань.

1.3. Поняття та види електронних доказів у цивільному судочинстві

Електронні докази та комп'ютерна експертиза є відносно недавніми доповненнями до засобів доказування в судовому процесі. На відміну від багатьох старих судово-медичних дисциплін, які часто вводилися в судовий процес без юридичних дебатів і перевірок, електронні докази викликали значну, і часто суперечливу, дискусію серед юристів. Різні правові системи по-різному відреагували на цей новий виклик. Деякі системи запровадили нове законодавство, яке конкретно стосується електронних доказів, як зробила це Україна декілька років тому. Інші системи намагаються встановити «найбільшу відповідність» існуючим доказовим концепціям і, де це можливо, застосовували існуючі правила аналогічно, наприклад, чи є електронний доказ прийнятним, залежить від того, чи був він подібним до доказу (паперового) документа чи доказу шляхом візуального огляду. Більшість систем використовують комбінацію обох стратегій. Там, де вводиться нове законодавство, акцент робиться на відмінності між електронними та традиційними формами доказів. Це може перешкодити

юристам використовувати свій колективний інституційний досвід для оцінки та інтерпретації таких доказів, що часто створює відчуття плутанини та невизначеності. Там, де використовуються аналогічні підходи, акцент робиться на подібності між традиційними та електронними доказами, а це, у свою чергу, може призвести до неналежного застосування правил доказування. У будь-якому випадку юристам важливо знати про відмінні характеристики електронних доказів, щоб вони могли впевнено та надійно оцінити використання електронних доказів.

Визначити, що ми маємо на увазі під «електронними» доказами, непросте завдання. Тип доказів, з якими ми маємо справу, також описується як «цифровий доказ» або «комп'ютерний доказ». Усі три терміни виражають деякі аспекти того, що цей тип доказів має деякі відмінні риси, які дозволяють виділити його серед інших засобів доказування. Однак визначити, що це за відмінні риси, далеко не просто. Швидкі технологічні зміни у сфері інформаційних технологій означають, що будь-яке визначення, вузько пристосоване до поточного стану технологій, ризикує швидко застаріти. Визначення, які належним чином підходять для майбутнього, навпаки, мають тенденцію бути надто абстрактними та перетинатимуть традиційні поділи та категорії в законодавстві про докази у різних країнах [2].

Існують різні визначення електронних доказів. До них належать «інформація, що має доказову силу, яка зберігається або передається у двійковій формі» та «інформація, яка зберігається або передається в електронній формі, на яку можна покладатися в суді». У своєму трактаті Е. Кейсі визначає електронні докази як будь-які дані, збережені або передані за допомогою комп'ютера, які підтверджують або спростовують теорію про наявність або відсутність певного факту [120].

Міжнародна організація з комп'ютерних доказів G8 запропонувала принципи процедур, пов'язаних із цифровими доказами (IOCE 2000). Хоча увага в цьому визначенні приділяється кримінальним розслідуванням, це

ширше визначення, ніж попередні визначення, і воно корисно пояснює певні важливі аспекти електронних доказів. Наприклад, посилання на «дані» стосується інформації, яка зберігається в електронній формі, такої як текст, зображення, аудіо- та відеофайли. Крім того, слово «комп'ютер» слід розуміти в його найширшому значенні та включати в нього будь-який пристрій, який зберігає, обробляє або передає дані. Крім того, визначення має на увазі, що докази мають бути належними та допустимими.

Щоб запропонувати ширше визначення, яке включає цивільні та кримінальні справи, ми пропонуємо таке визначення: електронні докази – це дані (включаючи вихідні дані аналогових пристроїв або дані в електронній формі), які обробляються, зберігаються або передаються будь-яким виготовленим пристроєм, комп'ютером чи комп'ютерною системою або передаються через систему зв'язку, які можуть скласти фактичну інформацію про будь-який факт.

Це визначення складається з трьох елементів. По-перше, посилання на «дані» включає всі форми доказів, створених, оброблених або збережених у пристрої, який у найширшому значенні можна вважати комп'ютером. По-друге, визначення включає різні пристрої, за допомогою яких дані можуть зберігатися або передаватися, у тому числі аналогові пристрої, які створюють вихідні дані. В ідеалі це визначення включатиме будь-яку форму пристрою, чи то комп'ютер, як ми зараз розуміємо в значенні комп'ютера, телефонні системи, бездротові телекомунікаційні системи та мережі, такі як інтернет, і комп'ютерні системи, вбудовані в пристрій, такі як мобільні телефони, смарт-карти та навігаційні системи. По-третє, визначення обмежує дані інформацією, яка має відношення до судового процесу, за допомогою якого суддя вирішує спір, незалежно від характеру розбіжностей, незалежно від форми та рівня рішення.

Електронним доказом може бути будь-який електронний файл із цифрового джерела. Це включає електронну пошту, текстові повідомлення, миттєві повідомлення, файли та документи, витягнуті з жорстких дисків,

електронні фінансові операції, аудіофайли та відеофайли. Спробуємо проаналізувати деякі з них.

Особливо важливою формою доказу в усіх розвинутих правових системах є документ. Отже, електронні документи є особливо важливою формою електронних доказів. Вони також є особливо гарним прикладом для ілюстрації деяких відповідних характеристик електронних доказів. Через важливість документів для нашого повсякденного життя та те, як ми працюємо з ними як папками, документами та фотокопіями, під час роботи з електронними документами багато найважливіших програм навмисно імітують «вигляд і відчуття» традиційних паперових документів. Тому ми створюємо електронні об'єкти, які називаються документами, що мають такий самий візуальний вигляд, як і документи, надруковані на папері, «гортаємо» їхні «сторінки» (як у деяких електронних пристроях для читання електронних книг і електронних журналів), «поміщаємо» їх у файли та папки та видаляємо їх у паперові кошики [60].

Електронна пошта також навмисно імітує традиційний лист, від значка листа на папці «Вхідні» до значка олівця, щоб «писати», а не вводити новий лист. Це неавтентичне знайомство може створити оманливе враження, що електронний документ існує десь на комп'ютері як єдине завершене ціле й зберігає свою структурну цілісність, навіть коли файл закрито або комп'ютер вимкнено, так само, як паперовий документ продовжує існувати, коли ми кладемо його в папку.

Цей надто наївний погляд недооцінює відмінності між електронними та паперовими документами, а також потенційно переоцінює їхню надійність. Однак може статися і зворотне, коли більш досвідчений користувач бачить процеси, які навмисно створюють вигляд паперового документа, і відкидає всі електронні докази як по суті оманливі, фальшиві та ненадійні, а не як новий вид документа. Це стає особливою проблемою для тих юрисдикцій, чие законодавство про докази має формальні визначення «документів» і «підтвердження за документами», як, наприклад, німецьке «Urkundenbeweis».

У цих юрисдикціях юридичні, а не фактичні питання можуть збільшити прірву між електронними та традиційними документами та вимагати доповнення законодавства, необхідного для того, щоб електронні документи також були «документами в законі».

Кращим і реалістичнішим підходом є визнання того, що документи в електронній формі мають особливі характеристики, які впливають як на перевірку автентичності (або походження), якщо автентичність виникає питання, так і на те, як електронні докази захищені та обробляються на судовому розгляді. Можна стверджувати, що докази в електронній формі повинні підлягати більш суворому механізму, ніж звичайні документи, що зберігаються на фізичному носії. Джон Д. Грегорі зауважив, що цілісність фізичних документів «часто захищається досить випадково», але цього не можна сказати про документи, які створюються, змінюються, передаються, зберігаються та видаляються в електронній формі [15]. Наприклад, судовий експерт може проаналізувати хімічні властивості чорнила на паперовому документі, щоб визначити, чи використовувалося більше ніж одне приладдя для письма, чи відповідає чорнило часу, коли ймовірно був створений документ, або матеріал властивості паперу. Після того, як документ буде написаний, зміни також залишать фізичні сліди. Тому з паперовими документами ми маємо чітке розуміння між оригіналом та його копіями, яке зазвичай визначається в законодавстві про докази. Це об'єкти з різними фізичними властивостями. Ця важлива відмінність стає проблематичною в електронному середовищі, де не тільки копію та оригінал неможливо розрізнити, але й сам акт роботи над «документом» автоматично й регулярно без відома автора створюватиме численні копії на комп'ютері, копії, які можуть зберігатися і записуватися попередні чернетки, навіть коли документ завершено. Документи в електронній формі мають низку особливостей, які створюють особливі труднощі, ніж паперові [212].

Хоча існують відмінності у форматі між неелектронною версією доказу та його електронним еквівалентом, але якщо відмінності не є суттєвими, суди не відхилятимуть електронні докази на користь інших форм доказів.

Відмінності можуть бути суттєвими залежно від фактів, про які йдеться: альтернативне представлення даних в електронній формі, у зрозумілій людині формі на екрані чи на друкованому аркуші паперу може стати суттєвим. У Мейнарді, США, суд відмовився прийняти роздруківку, яка нібито вказує на дату та час, коли відповідач отримав доступ до даних, що зберігаються в комп'ютері, на підставі того, що не всі дані, які були очевидні на екрані комп'ютера, були повністю відтворені на роздрукованому вигляді. У клопотанні про перегляд рішення суду суддя підтримав рішення, він зазначив, що якби всі дані були доречними, сторона позивача могла б записати дані на екран відео. У цій справі було продемонстровано, що інформація, записана на роздруківці, була неповною та не була точним відтворенням даних.

Традиційні документи дозволяють читачеві легко отримати доступ до інформації через тривалий час після її створення з невеликими додатковими витратами або взагалі без них. Єдине, що потрібно, це хороший зір або пристрій для читання тексту людині та знання мови, якою складено документ. Це дозволяє нам отримати доступ до інформації, наприклад, що зберігається в стародавніх рукописах і сувоях. Дані в електронній формі, навпаки, залежать від апаратного та програмного забезпечення. Дані потребують інтерпретатора, щоб увімкнути їх у формат, зрозумілий людині. Користувач не може створювати або маніпулювати електронними даними без відповідного обладнання. Електронний документ краще розуміти як процес, за допомогою якого незрозумілі фрагменти даних, які поширюються на носії інформації, збираються, обробляються та стають читабельними для людини. У цьому сенсі електронний документ існує незалежно від процесу (програмного забезпечення), який відтворює його за допомогою пристрою (апаратного забезпечення) кожного разу, коли користувач відкриває його на

екрані. Якщо ці електронні документи були створені в 1990-х роках, багато тисяч цих програм зараз більше не доступні для користування, і навіть якби таке програмне забезпечення було доступне, його було б неможливо завантажити в сучасну операційну систему. Додаткова проблема для старих даних полягає в тому, що для читання даних може знадобитися спеціальна машина із завантаженим спеціальним програмним забезпеченням. Це може спричинити додаткові витрати для сторони, як у випадку *RHE, Incorporated dba Adam & Eve v Department of Justice*, де RHE було наказано переглянути інформацію, що міститься в базі даних, навіть незважаючи на те, що не існувало жодної програми, яка б дозволила їм отримати запитувану інформацію.

Дані в електронній формі мають бути переведені в зручну для читання форму за допомогою набору технологій. Це означає, що виникають відмінності в тому, як той самий вихідний об'єкт відображається в різних ситуаціях. Хорошим прикладом, який є спільним для всіх користувачів інтернету, є те, що вебсайт може виглядати дуже по-різному залежно від того, який тип екрана та який браузер використовується, серед іншого. Як наслідок, не може бути концепції єдиного остаточного представлення конкретного вихідного цифрового об'єкта. Це може мати очевидні правові наслідки. Недбало складений електронний контрактний документ може неофіційно посилатися на «параграфи» документа без їх переліку, оскільки форматування на комп'ютері автора робить їх чітко видимими через розриви рядків у тексті. Ці дані форматування, надіслані покупцеві електронною поштою та відкриті на його комп'ютері за допомогою іншої програми, можуть бути нечитабельними, а абзаци – непомітними. Інший приклад можна знайти у змінених представленнях «емодзі» (ідеограм, що використовуються в електронному повідомленні, схожих на старіші смайли ASCII). Наприклад, у 2016 році Apple суперечливо змінила емодзі «ручний пістолет» на емодзі «водяний пістолет». Однак, коли повідомлення, що містить цей емодзі, надсилається на пристрій стороннього виробництва, воно

може відображатися на комп'ютері одержувача як мультяшне зображення справжньої зброї [217].

На відміну від електронних доказів, простий акт запуску комп'ютера та відкриття документа змінює його, наприклад, змінюючи його метадані. Різні спостерігачі, навіть незначно використовуючи різні механізми, відтворюють різні версії об'єкта, про який йде мова, і непросто вирішити, яку з них слід вважати «більш автентичною».

Щоб впоратися з цією проблемою, можливо, ми можемо використати підхід, використаний на основі свідчень очевидців. Ми знаємо, що різні очевидці однієї події завжди нададуть дещо різні пояснення того, що сталося. Подібно до того, як ми намагаємося мінімізувати ці наслідки за допомогою відповідних протоколів і процедур — наприклад, для групи людей, яка може включати сторони або свідків — протоколи та процедури, які використовує професіонал із електронних доказів, можуть мінімізувати, але не усунути викривлення, яке створюється при дослідженні. Це означає, що вкрай важливо визначити відповідні стандарти, протоколи, контрольні показники та процедури, а також відповідне апаратне та програмне забезпечення щодо управління та використання будь-якого елемента електронного доказу.

Технології швидко змінюються в операційних системах, прикладному програмному та апаратному забезпеченні. У результаті дані в електронній формі можуть досягти точки, коли їх неможливо буде прочитати, зрозуміти або використовувати з новим програмним або апаратним забезпеченням. Наприклад, компанія, що займається програмним забезпеченням, може більше не виробляти програмне забезпечення, яке є зворотно сумісним або «сумісним із попередніми версіями» (де нові версії програмного забезпечення можуть працювати зі старішими продуктами). Технічна застарілість є серйозною проблемою, яка впливає на кожен аспект судового процесу, особливо тому, що швидкість змін стала настільки швидкою.

Невпинна швидкість змін має ще один наслідок, який знову ж таки найкраще пояснюється порівнянням електронних доказів із традиційними.

Свідчення очевидців є одним із найстаріших, якщо не найстарішим, видом доказів, що використовується в суді. Незважаючи на це, спосіб отримання та інтерпретації пояснень свідків у судочинстві мало змінився протягом століть, і правові системи регулярно зберігають культурно застарілі поняття, такі як присяга або ідентифікація документів, через їхню ритуальну цінність. Докази відбитків пальців набагато молодші, їх використання трохи більше ста років. З моменту створення, незважаючи на те, що основи дисципліни залишилися незмінними, було внесено важливі зміни в спосіб інтерпретації доказів відбитків пальців, а також особливості, які ми шукаємо під час встановлення відповідності. Експерту з відбитків пальців, який навчався 90 років тому, ймовірно, знадобиться принаймні курс підвищення кваліфікації. Докази ДНК ще молодші, але за їх 30-річну історію відбулися значні зміни в способах збору, аналізу та інтерпретації ДНК. Експерт, який отримав підготовку в 1980-х роках, потребував би значної перепідготовки, щоб мати змогу працювати з сучасними технологіями та обладнанням. Для електронних доказів темпи змін ще швидші. Це ще більше ускладнює інформування юристів та інших неспеціалістів про відповідні події та збільшує довіру до експертів. Це також означає, що важливо, щоб експерт мав сучасні знання та проходив постійне навчання, яке важливіше, ніж «досвід» у цій галузі.

Проблемою, пов'язаною зі швидкими змінами з часом, є горизонтальна диверсифікація програмного та апаратного забезпечення. Якщо ДНК-експерт аналізує зразок крові, йому не обов'язково знати заздалегідь вік, національність або стать донора. На відміну від цього, фахівець із електронних доказів повинен знати та пройти підготовку щодо конкретного типу пристрою та програмного забезпечення, які йому пропонують проаналізувати [109].

Отримати відповідні електронні інструменти для експертного аналізу пристрою може бути складно з двох причин: по-перше, інструменти ще належить розробити, а по-друге, тому що такі інструменти можуть бути дорогими.

Електронні докази також повинні бути засвідчені, як і будь-які інші форми доказів. Докази автентифікації для електронних доказів ще важливіші, й іноді можуть бути складними. Безсумнівно, використання технологій забезпечило нам зручність і ефективність. Але якщо сторони вирішують використовувати результати технологій, вони також повинні визнати необхідність доводити автентичність і цілісність доказів, отриманих за допомогою технології, навіть якщо вартість такого доказу може вважатися високою. Це особливо стосується випадків, коли докази автентифікації проливають світло на приховані припущення та приховані помилки, властиві електронним доказам, які можуть вплинути на точність самого електронного доказу [59].

Це не означає, що докази автентифікації завжди повинні надаватися для кожного доказу. У цивільному судочинстві в Англії та Уельсі вважається, що сторона визнає автентичність документа, оприлюдненого відповідно до положень Правил цивільного судочинства 31, якщо не буде надіслано повідомлення про те, що сторона бажає, щоб документ було доведено в суді. Таким чином, якщо автентичність документа ставиться під сумнів, сторона, яка порушує питання, повинна зробити це на ранній стадії провадження, таким чином надаючи стороні, яка подає документ, можливість зібрати докази для підтвердження правдивості документа.

Електронними документами легко маніпулювати: їх можна копіювати, змінювати, оновлювати або видаляти. Інтеграція телекомунікацій і комп'ютерів для формування комп'ютерних мереж (таких як глобальні мережі та інтернет) додатково дозволяє створювати та обмінюватися даними в набагато більших обсягах, ніж це було можливо досі, і через фізичні та географічні кордони. По суті, електронна пошта, обмін миттєвими повідомленнями та інтернет-комунікації є дубльованою та розподіленою технологією. Коли комп'ютери об'єднано в мережу таким чином, електронний документ може бути передано, а численні копії розповсюджені по всьому світу дуже швидко. Наприклад, у справі AMP проти невідомих

осіб мобільний телефон позивача було вкрадено або втрачено. Він не був захищений паролем. У телефоні зберігалася низка фотографій, деякі з яких мали відвертий характер. Невдовзі після зникнення або викрадення телефону цифрові зображення були завантажені на різні веб-сайти соціальних мереж, що дозволило іншим завантажувати та ділитися зображеннями. Деякі із сайтів соціальних мереж видалили зображення на запит, але зображення були заправлені на шведський вузол BitTorrent і продовжували поширюватися. Суддя вирішив, що позивач має право на тимчасову судову заборону, щоб запобігти розповсюдженню цифрових зображень або шляхом звичайного завантаження з сайту, або шляхом завантаження за допомогою протоколу BitTorrent. Заборона була надана в наступних умовах:

- негайно припинити завантаження будь-якого BitTorrent, що містить будь-яку частину або частини файлів, перелічених у Додатку С цього Наказу;
- не можна завантажувати або передавати будь-якій іншій особі будь-яку частину або частини файлів, перелічених у Додатку С цього Наказу;
- не повинні створювати жодних похідних файлів, перелічених у Додатку С цього Наказу;
- не повинні розголошувати ім'я Позивача (або будь-яку іншу інформацію, яка може призвести до її ідентифікації) або назви будь-яких файлів, перелічених у Додатку С цього Наказу [16].

Простота передачі та копіювання електронних документів збільшила потенційний обсяг даних, які необхідно ідентифікувати, щоб отримати відповідні документи, що стосуються судового процесу. Наприклад, у рамках перевірки Enron Федеральна комісія з регулювання енергетики оприлюднила набір даних, що містить 500 МБ повідомлень. Проте «традиційні» повідомлення, подібні до цих, становлять мізерну меншість усіх електронних даних (і потенційних доказів), які регулярно створюються машинами, як-от моніторинг і маршрутизація інтернет-трафіку. На додаток до величезного обсягу цих даних, це створює додаткову проблему, оскільки в необробленому вигляді вони не зрозумілі людям - більшість даних є

інструкціями, які надсилаються між машинами та для використання ними. Для того, щоб перетворити їх на докази для судових проваджень, потрібен значний обсяг перекладу або роботи експерта відповідної кваліфікації.

Щоб ефективно працювати з такою кількістю даних, регулярно знадобляться інші комп'ютерні інструменти, такі як програмне забезпечення для аналізу даних. Ці методи аналізу несуть свої власні проблеми щодо точності, надійності, шкідливого впливу тощо. Програмне забезпечення для аналізу посилань, наприклад, може створити з цих даних картину мережі, яка показує, як люди в компанії сформували кола спілкування, які можна витлумачити як ядро, просто як результат того, як програмне забезпечення організувалось і візуалізує інформацію. З іншого боку, інші судово-медичні дисципліни регулярно використовують науково підтверджені методи вибірки. Наразі все ще існує тенденція не використовувати однакові протоколи вибірки принаймні для деяких типів електронних доказів, зокрема для тих типів даних, які в принципі можуть бути оцінені безпосередньо людьми. Це може змусити свідків, візуально оглянути потенційно великі обсяги тривожних незаконних матеріалів. Однак деякі юрисдикції почали використовувати статистичні методи (електронного) збору доказів більш систематично. «Прогнозне кодування» або «перевірка за допомогою технології» використовує баєсівську теорію ймовірності та машинне навчання для сканування електронних документів на наявність даних, що стосуються справи, і автоматично визначає «хороших кандидатів» для подальшого вивчення людьми. Це кодування в основному для цивільного електронного аналізу або виявлення, що отримало схвалення судів у 2016 році в Англії [29].

Можливість швидкої передачі доказів також може створити проблеми, пов'язані з юрисдикцією. Зараз багато користувачів комп'ютерів регулярно завантажують усі свої файли з метою резервного копіювання до інтернет-провайдерів. Бізнес дані можуть оброблятися за допомогою технології «хмарних обчислень», яка передбачає передачу даних стороннім серверам,

які не належать і не контролюються компанією та, можливо, розташовані по всьому світу, при цьому кожен сервер у будь-який час зберігає лише фрагменти даних. З іншого боку, автоматичне завантаження даних також означає, що користувач пристрою втрачає контроль над інформацією, яку він створив. Видалити або позбутися інформації може стати дедалі складніше, якщо її було створено на пристрої та завантажено в «хмару» [36].

Метадані - це, по суті, дані про дані. Наприклад, метадані стосовно аркуша паперу як фізичного документа можуть бути такими:

- явні від перегляду самого паперу, як-от назва документа, дата, передбачуване ім'я особи (осіб), яка його написала, хто його отримав і місцезнаходження документа;

- неявні, які включають такі характеристики, як типи використовуваного типу (шрифту), як-от жирний, підкреслений або курсив, розташування документа, наприклад, кольоровий файл для позначення певного типу документа, і мітки документа, які також діють як покажчики. щоб дозволити особі, яка використовує документ, працювати з ним певним чином, наприклад, конфіденційним файлом.

Усі документи в електронному форматі містять метадані в тій чи іншій формі, включаючи повідомлення електронною поштою, електронні таблиці, вебсайти та документи для обробки текстів. Насправді електронний документ повинен мати метадані, які допоможуть інтерпретувати призначення електронного документа. Такі дані можуть включати та автоматично братися з вихідного прикладного програмного забезпечення або надаватися особою, яка спочатку створила запис. Список доступної інформації включає, але не обмежується такими даними: коли та як було створено документ (передбачуваний час і дата), тип файлу, ім'я передбачуваного автора (хоча це не обов'язково буде достовірним), розташування, з якого файл було відкрито або де він зберігався, коли файл відкривався востаннє (передбачуваний час і дата), коли він востаннє змінювався, коли файл востаннє зберігався, коли він востаннє друкувався,

ідентифікатор передбачуваних попередніх авторів, розташування файлу кожного разу, коли він зберігався, відомості про те, хто ще може отримати доступ до нього, й, у випадку електронної пошти, адреси прихованої копії (bcc).

Оскільки метадані зазвичай створюються автоматично програмним забезпеченням і без відома користувача, їх також складніше змінювати, маніпулювати чи видаляти. Уявіть, що особа пише документ на комп'ютері. Програмне забезпечення додасть метадані, пов'язані з цим документом, наприклад, час створення документа. Файл, у якому зберігається ця інформація, є метаданими, які записують час події запису. Оскільки це не навмисне створення автором, а автоматичний факт, створений програмним забезпеченням, який часто невидимий для користувача, він може не знати про ці дані, а навіть якщо й знав, може не знати, як їх змінити чи видалити.

Однак слід сказати, що метадані не є безпомилковими. Його інтерпретація вимагає необхідності робити припущення щодо середовища, в якому вони були створені. Якщо час на пристрої був неточним (наприклад, ноутбук перелітав через часові пояси без налаштування на це, або годинник повільний, або його навмисно змінено), записані метадані будуть хибними. Оскільки в цьому сенсі середовище може «брехати», поінформовані спеціалісти можуть навмисно маніпулювати даними. Наприклад, досвідчені фішингові особи, які використовують електронну пошту, не лише підроблять адресу відправника електронних листів, які вони надсилають, але й маніпулюють усім заголовком, щоб приховати місце, звідки походить електронний лист. Нарешті, оскільки метадані є ненавмисним створенням інформації, експерти або інші треті сторони, які працюють у тому самому середовищі, також створюватимуть метадані, і таким чином потенційно забруднюють докази. Недбалий фахівець із електронних доказів або ІТ-адміністратор компанії, якого співробітник попередив про потенційно недобросовісну діяльність, може самим актом відкриття та перегляду файлу створити нові метадані та перезаписати старі (новий час, коли документ був,

згідно з комп'ютером, створений), таким чином видаливши потенційно корисні метадані про незаконну діяльність, наприклад фактичну дату та час її вчинення.

У загальному плані існує три основних типи метаданих:

1) Описові метадані описують ресурс для певної мети, наприклад, для розкриття чи відкриття. Метадані можуть включати таку інформацію, як назва, ключові слова, анотація та ім'я особи, яка претендує на роль автора. Щоб більш повно зрозуміти історію документа, необхідно було б отримати інформацію про те, як і коли система записала ім'я передбачуваного автора.

2) Структурні метадані описують, як ряд об'єктів об'єднуються. Деякі приклади структурних метаданих включають «ідентифікацію файлу» (наприклад, для ідентифікації окремого розділу, який є частиною книги або звіту), «кодування файлу» (для ідентифікації кодів, які використовувалися щодо файлу, включаючи стандарт кодування даних). використовуваний (наприклад, ASCII), метод, який використовувався для стиснення файлу, і метод шифрування, якщо він використовується), «відтворення файлу» (щоб визначити, як файл був створений, включаючи таку інформацію, як програмне забезпечення, операційна система та обладнання), «структура вмісту» (для визначення структури вмісту запису, наприклад, визначення набору даних, словник даних, файли з кодами повноважень тощо) і «джерело» (для ідентифікації відповідних обставини, які призвели до збору даних).

3) Адміністративні метадані, які надають інформацію для допомоги в управлінні ресурсом. Адміністративні дані далі поділяються на метадані керування правами та метадані збереження чи ведення записів [176].

Метадані можуть бути фундаментально пов'язані з електронним документом і бути його частиною, включені в системи, що використовуються для створення документа, або пов'язані з ним з окремої системи. Метадані можна переглядати різними способами, одним із яких є перегляд «властивостей» в програмі, яка створила документ, або за допомогою

програмного забезпечення, спеціально створеного для цієї мети. Деякі метадані також можна видалити за допомогою спеціального програмного забезпечення. Це може бути корисним під час надсилання файлів третім особам, але може спричинити додаткові витрати, якщо суд накаже надати дані в оригінальному форматі, як у випадку *Williams v Sprint/United Management Company*. Перш ніж передати позивачам електронні табличні документи у формі Excel, Sprint змінив електронні файли, зокрема видаливши метадані з електронних файлів, які включали електронні таблиці, і заборонив одержувачам переглядати певні дані, що містяться в електронних таблицях, заблокувавши значення певних клітин. Sprint було наказано створити електронні таблиці в тому вигляді, у якому вони підтримувалися, включаючи метадані, хоча несприятливі аналізи та номери соціального страхування можна було відредагувати, а також було наказано створити розблоковані версії електронних таблиць. У своєму рішенні суддя обговорював метадані та те, чи є вони достатньою частиною документа в електронному форматі для його передачі іншій стороні [227].

Ця програма ілюструє важливість метаданих, пов'язаних із електронним об'єктом. Документи в електронній формі зазвичай включають метадані, і за таких обставин одержувачу здається нереалістичним відмовитися надати повний документ, включаючи пов'язані метадані.

Значна кількість електронних даних створюється через спілкування між людьми, розділеними географічними, політичними, соціальними та культурними кордонами. У той час як інтернет залучав людей, раніше розділених відстанню, до взаємодії, він також створює нову форму «відстані» між комунікантами. Деякі способи спілкування погано підходять для цього нового середовища, наприклад не відображається вираз обличчя та тон голосу. Однак докази мають значення і їх можна інтерпретувати лише зі знанням контексту, в якому воно було створене. Повідомлення «Я вас усіх ненавиджу й бажаю, щоб ви померли» між підлітком і його батьками щодо прибирання кімнати буде сприйматися більшістю людей, знайомих із

подібною культурою, як незначне й несерйозне. Ті самі слова, які містяться в ретельно написаному листі, матимуть інше значення. Таким чином, слід розглянути, чи електронний лист, повідомлення в Twitter або повідомлення на дискусійному форумі більше схоже на доказ чи на прямий словесний обмін.

Суд має розглянути соціальний контекст, в якому слід розуміти електронні докази, щоб рішення було правильним. Візуальна форма, в якій з'являється це свідчення, може не відображати правдивого соціального значення, яке було повідомлено користувачам під час створення. Наприклад, твіт може виглядати як попередження, але його точно не сприймають учасники. Оскільки судді та присяжні часто мають дуже різний технологічний досвід, виникає спокуса надати соціологічні чи психологічні докази з цих питань, але процесуальні правила щодо прийнятності цілком можуть цьому перешкодити. Однак ці питання виходять за межі компетенції спеціаліста з електронних доказів, який не має жодної позиції щодо них.

Як правило, носії, на яких зберігаються електронні дані, є крихкими. Електронні носії інформації за своєю суттю нестабільні, і якщо носії не зберігаються належним чином, вони можуть швидко зіпсуватися без зовнішніх ознак псування. Дані також піддаються ризику випадкового чи навмисного пошкодження та випадкового чи навмисного видалення.

Зараз комп'ютери та системи працюють переважно в мережевому середовищі. Мережевий світ включає пристрої (MP3-плеєри, комп'ютери, портативні комп'ютери, мобільні телефони, персональні цифрові помічники (КПК) і планшети), пов'язані за допомогою програм (факсимільні передачі, голос через інтернет-протокол (VoIP), електронна пошта, однорангове програмне забезпечення) й обмін миттєвими повідомленнями), які працюють через мережі (інтернет, інтранет, бездротові мережі, стільникові мережі та комутований доступ). Природа цього налаштування полягає в тому, що майже все, що будь-хто робить на пристрої, підключеному до мережі, можна поширювати та дублювати з неперевершеною легкістю. У результаті один і

той самий елемент електронних даних може перебувати практично будь-де. Наслідки для юристів і практиків очевидні. Відповідний документ може бути доступним, але може бути незрозуміло, де він знаходиться. Це впливає на те, як ведеться збирання доказів, і на те, скільки зусиль доведеться докласти учаснику цивільної справи, щоб знайти відповідні документи для виявлення чи розкриття.

Приклад зі Сполучених Штатів Америки служить для ілюстрації деяких проблем, з якими стикається велика організація при пошуку відповідних документів в електронному форматі, особливо електронної пошти, яка використовувалась давно. Зубулаке, директор і старший продавець UBS Warburg LLC, почала судовий процес за гендерну дискримінацію, коли її звільнили з роботи. Серед іншого, вона стверджувала, що її менеджер Чапін ставився до неї інакше. Вона вимагала розкриття електронної пошти UBS для підтвердження своїх дій. Сторони не погодилися щодо ступеня розголошення електронних листів, хоча не заперечувалося, що електронна пошта була важливим засобом спілкування, оскільки кожен продавець отримував приблизно 200 електронних листів щодня. Положення Комісії з цінних паперів і бірж вимагали від UBS зберігати електронні листи. UBS використовувала два методи зберігання: резервні стрічки для аварійного відновлення та оптичні диски. Це означало, що було три можливі місця, де можна було знайти відповідні електронні листи: у файлах, якими користувалися співробітники, електронних листах, заархівованих на оптичних дисках, і електронних листах, надісланих зареєстрованому трейдеру та від нього (внутрішні електронні листи не записувалися), які зберігалися на оптичних запам'ятовуючих пристроях. Дев'яносто чотири резервні стрічки було визначено як відповідні для цілей розкриття інформації. UBS використовувала програму резервного копіювання, яка робила знімок усіх електронних листів, які існували на певному сервері на момент створення резервної копії; а саме в кінці кожного дня, кожної п'ятниці ввечері та в останній робочий день місяця. Оскільки резервні копії

електронних листів періодично створювалися, деякі електронні листи не зберігалися, зокрема, коли користувач отримав або надіслав електронний лист і видалив його того самого дня. Суддя вирішив, що Зубулаке має право на розкриття електронних листів, оскільки вони стосуються її претензії. UBS було наказано створити всі відповідні електронні листи, які існували на оптичних дисках або серверах за власний рахунок, а також з п'яти резервних стрічок, вибраних Zubulake. Консалтингова фірма відновила та обшукала записи за 11 524,63 доларів США. Додаткові витрати включали час, який знадобився юристам для перегляду електронних листів, що призвело до загальної вартості 19 003,43 доларів США. Було виявлено близько 1541 відповідних електронних листів. На оптичних дисках було знайдено менше 20 відповідних електронних листів. У липні 2003 року Zubulake подала нову заявку на реставрацію та пошук решти резервних стрічок. UBS підрахувала, що вартість становитиме 273 649,39 доларів США, і подала заявку на перенесення витрат на Zubulake. Розглядаючи семифакторний тест (який не має значення для цілей цього конкретного обговорення), суддя зазначив, що значна кількість відповідних електронних листів існувала на резервних стрічках, і були докази того, що фірма видалила відповідні електронні листи. Суддя вирішив, що Зубулаке має заплатити 25 відсотків вартості відновлення резервних стрічок. UBS повинні були сплатити всі інші витрати.

Мета опису цього кейсу полягає в тому, щоб проілюструвати проблеми, з якими стикаються багатонаціональні організації при пошуку відповідних доказів в електронній формі. Природа розподіленого середовища означає, що почала виникати низка практичних проблем у визначенні того, який матеріал потрібно розкрити або відкрити іншій стороні. По-перше, необхідно запобігти знищенню доказів, а потім необхідно встановити, де ймовірно знаходяться докази, перш ніж розпочинати шукати з різних джерел для виявлення відповідних документів. Це завжди вимагатиме від сторони визначення місця розташування всіх резервних стрічок, незалежно від того, чи зберігаються вони в приміщенні, у третіх сторін у віддаленому сховищі за

межами сайту або на окремих комп'ютерах, серверах, в архіві чи системі аварійного відновлення. Типи носіїв інформації, які необхідно буде ідентифікувати та знайти, включають стрічки, диски, накопичувачі, USB-накопичувачі, iPad, ноутбуки, ПК, КПК, мобільні телефони, пейджери та аудіосистеми (включаючи голосову пошту) і це лише деякі з них. Крихкість і всюдисущість електронних накопичувачів зробили сучасні відкриття грізним процесом.

На відміну від обговорення вище, діапазон доказів у електронній формі величезний, і він включає не лише роздруківки того, що можна було б назвати звичайними файлами, такими як копії листів, контрактів або електронних таблиць. Інші форми цифрових документів включають звіти з комп'ютерних баз даних, електронні записи транзакцій і цифрове зберігання та відтворення зображень, таких як скановане зображення оригінального паперового документа. Обробка доказів у цифровій формі потребує різних і часом складних міркувань.

Крім того, використання електронного пристрою не завжди вимагає «оригінального документа». Якщо «оригінальний документ» створюється в електронній формі, але ніколи не зберігається більш постійним, неефемерним способом, «оригінальний» цифровий «документ» припиняє своє існування для будь-яких практичних цілей. Миттєвий обмін повідомленнями є прикладом доказів, які можуть не зберігатися, що робить його аналогом усної розмови.

Проблеми можна додатково розглянути за допомогою наступної розширеної ілюстрації. Наприклад, оригінал фізичного документа, такого як комерційний контракт між двома сторонами, підписаний уповноваженими представниками обох сторін і визнаний оригіналом, є основним доказом змісту контракту. Навіть якщо договір було створено на комп'ютері, фізичний документ все одно буде оригінальним документом, оскільки його підписали та прийняли обидві сторони. Однак, якщо договір, за яким згодом діють обидві сторони, існує лише в електронній формі на комп'ютері,

основним доказом документа буде електронний контракт, який зберігається на ідентифікованому комп'ютерному запам'ятовуючому пристрої, такому як жорсткий диск комп'ютера. Друк документа на папері забезпечить отримання копій у формі, зрозумілій людині, яка, у свою чергу, міститиме вторинні докази документа.

У виняткових випадках докази, записані на відео та на магнітофонну плівку, можуть використовуватися замість свідчень. У цивільному судочинстві докази можуть надаватися за допомогою відеозв'язку або будь-яким іншим способом за умови отримання дозволу суду.

Камери відеоспостереження є невід'ємною частиною життя двадцять першого століття, відтоді як основи їх використання були закладені в останні десятиліття двадцятого століття. Докази зображень із камер відеоспостереження можуть бути дуже корисними для ідентифікації осіб та встановлення певних фактів. Такі докази були прийняті в англійських судах. Широка доступність доказів, записаних на відео та на плівку, відкрила можливість того, що такі докази можуть бути доповнені більш досконалыми методами з покращенням звуків або зображень разом із використанням більш досконалих методів, таких як ідентифікація на слух і картографування обличчя, що можуть допомогти ідентифікувати осіб на записі.

Перш ніж використовувати такі докази, слід ретельно вивчити розглянуту технологію. Хорошим прикладом такого судового розгляду є те, що зроблено Стейном Ж. Дж. у справі Кларка (Роберт Лі), де суд проаналізував техніку картографування обличчя шляхом накладання відео. Суд ретельно розглянув надійність основних наукових методів, зазначивши, що методи самі по собі можуть бути придатними, а їх неправильне використання експертом у конкретній справі може, у свою чергу, вплинути на доказову силу таких доказів. Лише після того, як він був задоволений на цих двох підставах, докази ідентифікації від застосування техніки були прийняті.

Питання, що стосуються надійності та застосування цих методів, дуже важливі для дослідження доказів, залежно від характеру та складності кожного методу. Але можна отримати деякі вказівки, які впливають із найкращих практик роботи з електронними доказами. Наприклад, для доказових методів, які передбачають маніпулювання та покращення електронних зображень, Грегорі Джозеф зазначив, що перед тим, як розширені електронні зображення можна буде використати з користю, необхідно виконати наступні умови:

- Початкове зображення має бути належним чином підтверджено.
- Оригінальне зображення має залишитися недоторканим, щоб оригінал можна було порівняти з розширеною версією.
- Оригінальне зображення має бути збережено таким чином, щоб його цілісність не могла бути поставлена під сумнів.
- Процес покращення має бути повністю задокументований.
- Процес покращення має здійснюватися таким чином, щоб процес міг повторити інша сторона.
- Покращені зображення слід зберігати таким чином, щоб запобігти маніпуляціям із ними та зберегти їх цілісність [148].

Важливі уроки також були викладені щодо використання технологій і методів розпізнавання голосу для цілей ідентифікації у *R v Flynn and St John*. У цій справі намагалися ідентифікувати двох осіб як учасників за допомогою методів розпізнавання голосу. Виносячи рішення, суд зазначив, що існує дві категорії доказів розпізнавання голосу: експертні свідчення з використанням слухового аналізу або акустичного/спектрографічного аналізу, або свідчення непрофесійного слухача, коли непрофесійний слухач як свідок повинен володіти певними спеціальними знаннями про особу, що дозволяє йому розпізнати голос цієї особи. Такими свідками можуть бути близькі родичі або друзі. Суд також зазначив, що ідентифікація підозрюваного за допомогою розпізнавання голосу складніша, ніж візуальна ідентифікація, та що ідентифікація голосу експертами за допомогою складних слухових,

акустичних і спектрографічних засобів, а також складні аудіальні методи, ймовірно, будуть більш надійними, ніж ідентифікація неспеціалістом, і що якість ідентифікації непрофесійним слухачем дуже різна. Крім того, дослідження показали, що впевнене розпізнавання знайомого голосу непрофесійним слухачем все ж може бути помилковим, оскільки в той час як експерт може скласти загальний профіль мовленнєвих патернів індивіда в поєднанні з інструментальним аналізом і довідковими дослідженнями, реакція непрофесійного слухача є принципово непрозорою, тому що він не може знати та не має способу пояснити, на які аспекти мовленнєвих моделей мовця він реагує, і не має можливості оцінити значущість індивідуально спостережуваних особливостей відносно загального профілю мовлення [4].

Системи представлення електронних візуальних доказів (включаючи цифрові дисплеї, створені комп'ютером графічні презентації, анімаційну графіку та технологію захоплюючого віртуального середовища) використовувалися в судових процесах у багатьох юрисдикціях. Такі інструменти можна використовувати для представлення доказів та ілюстрації гіпотез, заснованих на наукових даних, або для зображення сприйняття свідка, або для ілюстрації того, що могло статися (бачене з певної точки зору) під час конкретного інциденту. Технологія цифрової реконструкції також може бути застосована в суді, щоб досліджувати та ілюструвати сценарії та запитання «а що, якщо», перевіряти конкуруючі гіпотези та виявляти будь-які можливі невідповідності та розбіжності в доказах [12].

Комп'ютерна анімація та інтерактивне віртуальне моделювання потенційно не мають собі рівних у своїх можливостях подання складних доказів. Використання таких сприятливих технологій візуалізації може вплинути на те, як глядач засвоює та співвідносить докази. У багатьох випадках візуальні медіа потенційно можуть допомогти зробити докази більш релевантними та легшими для розуміння. В інших випадках це може вважатися несправедливим упередженням членів журі [9].

На перший погляд, ці створені комп'ютером графічні реконструкції можуть розглядатися як потенційно корисні в будь-якому суді, і їх часто розглядають як будь-які інші форми цифрових доказів щодо їх допустимості. Зокрема, вони допускаються до складу показань експертів або як особливий вид речових доказів. Однак ця конкретна форма цифрових медіа потребує особливої обережності та уваги через її вроджену переконливу природу та надмірне довір'я, яке глядач може покласти на докази, представлені за допомогою середовища візуалізації, такого як цей. Це часто називають тенденцією «побачити – значить повірити» [97].

Оскільки суди все частіше починають використовувати мультимедійні та кінематографічні дисплеї, це має серйозні наслідки для судових процесів, які відбуваються і які внутрішньо пов'язані із застосуванням такої технології. Необхідно поставити під сумнів те, чи не впливає спосіб представлення доказів негативно на рішення, ухвалені в судах під час використання такої технології [203].

Однак, як можна побачити, незважаючи на ці відмінності, докази в електронній формі мають важливі риси, пов'язані з іншими типами доказів. Показання свідків, судово-медичні сліди, як-от ДНК, і докази за допомогою документів — усі вони можуть стати основою для аналогічних міркувань для визначення доказової цінності елемента електронного доказу. Професіонал із електронних доказів, однак, має іншу роботу, ніж робота аналітика ДНК чи судового ентомолога, і, зокрема, він має справу з математичними абстракціями, а не з емпіричними об'єктами. Тому його висновки, як правило, не будуть у формі відповідних ймовірностей або інших кількісно визначених узагальнених тверджень. «Універсальні» теорії доказів, на жаль, або рідкісні, або занадто абстрактні, щоб мати значну практичну цінність. Проте «ієрархія пропозицій», яку просуває Служба судової експертизи Великобританії, може створити таку структуру, яка також може допомогти глибше висвітлити відмінні риси електронних доказів і їх значення для практики. Ми можемо лише окреслити, як може виглядати розширення цієї

схеми на електронні докази. Ми вже неявно використали деякі їхні ідеї, наприклад, у визначенні електронних доказів. Щоб інтерпретувати докази, фахівець із електронних доказів (або суддя) має розглянути пропозиції, які представляють відповідно позивача чи відповідача. Вагомість доказів можна встановити лише за умови розгляду пропозицій обох сторін і врахування збільшення або зменшення ймовірності для обох.

РОЗДІЛ 2.

ЕЛЕКТРОННІ ДОКАЗИ В ЦИВІЛЬНОМУ СУДОЧИНСТВІ КРАЇН АНГЛО-АМЕРИКАНСЬКОЇ ПРАВОВОЇ СІМ'Ї

2.1. Практико-орієнтований підхід до електронних доказів у цивільному судочинстві США

Розмірковуючи про роль і значення електронної інформації у праві розвинених країн, сучасні дослідники намагаються відповісти на питання про те, чи є така інформація самостійним видом доказів. Таке питання цілком справедливе, оскільки вітчизняна правова система відноситься до романо-німецької правової сім'ї, якій властива, поряд з особливою юридичною значимістю нормативних актів, висока теоретична розробленість правових понять та термінів, про що буде йтися в наступному розділі.

Проте зовсім інший підхід щодо значення «електронної інформації» та зокрема «електронних доказів» використовується, коли йдеться про правову систему США, що належить до англосаксонської правової сім'ї, що характеризується великою роллю судового прецеденту при регулюванні суспільних відносин і суто прикладною юридичною доктриною [200, с. 145-146]. У цій правовій системі відсутнє чітке розмежування доказів на види, а доказове право згруповано за типовими для практики проблемними ситуаціями. Як стверджують самі американські правознавці, статутне доказове право США, по суті, є закріпленням найважливіших та знакових судових рішень, узагальненою практикою і носить заборонний характер, тобто вказує, в яких випадках доказ не може бути визнаним допустимим [200, с. 1]

За таких обставин питання про те, чи є «електронні докази» самостійним видом доказів, немає істотного значення для американських юристів. Останніх більше цікавлять конкретні порушення прав і законних інтересів громадян при використанні ними комп'ютерної інформації, тоді як

із юридичними поняттями вони обходяться вільніше. Звісно ж, що таке ставлення до правової термінології є причиною того, що термін «електронна інформація» чи «електронний доказ» широко використовуються в англomовній літературі, на відміну від континентальних досліджень, для яких властиве більш строге ставлення до понятійного апарату в цілому та до системи видів доказів зокрема [116, с. 26-27]

При цьому, якщо для представника романо-німецької правової сім'ї питання про введення в теорію нового поняття дозволяється, виходячи з якихось загальних критеріїв, вироблених тією чи іншою концепцією, то для американського дослідника зазначена проблема вирішується іншим чином: якщо те чи інше явище викликало проблеми в правозастосовній практиці, то одного цього, як правило, достатньо для появи нового терміна.

У зв'язку з цим «електронні докази» видаються американським юристам реальним правовим явищем, оскільки породжують велику кількість конкретних спірних ситуацій, вирішення яких відбувається за допомогою прийняття нормативних актів, і шляхом використання судових прецедентів.

Одне з визначень поняття «електронні докази» дав проект Evidence, який діє під егідою USAID, згідно з яким електронні докази – це будь-які дані, отримані від аналогового пристрою та/або цифрового пристрою потенційного значення, які генеруються, обробляються, зберігаються або передаються за допомогою будь-якого електронного пристрою. Цифрові докази – це електронні докази, які формуються або перетворюються в числовий формат. Це визначення важливе, оскільки воно уточнює різні визначення, запропоновані багатьма вченими, а також усуває деякі їх неясності, а також воно враховує всі можливі варіанти електронних доказів і демонструє глибоку міждисциплінарну природу цього поняття. Наведене вище визначення електронних доказів має більш широке застосування, ніж будь-які інші [82, с. 5].

Отже, електронні докази — це інформативний цифровий компонент, який приймає багато форм, наприклад електронний лист, зображення, аудіо

та фотографії, за допомогою яких можна пов'язати сторони, свідків, експертів та інших учасників справи.

Одним із найвідоміших визначень електронних доказів є наступне: «всі цифрові дані, за допомогою яких можна вирішити справу або довести зв'язок між стороною та фактом». Числові дані — це набір чисел із тексту, які включають письмові зображення, а також графіки, карти, аудіо та креслення [93, с. 25].

Завдяки наведеним вище визначенням електронні докази в США можна розділити на кілька підрозділів і класифікацій за різними критеріями.

По-перше, електронні докази можна класифікувати за типом (формою електронних даних) [226, с.3]. Сюди входять письмові повідомлення, наприклад документи, написані на комп'ютері, повідомлення, написані та надіслані електронною поштою, а також тексти, надіслані мобільним телефоном. Сюди також включається запис голосу. Їх можна записати та зберегти на мобільному телефоні або в додатку. А ось цифрові фотографії є втіленням візуальних фактів, роздрукованих або збережених у цифровому вигляді [177].

Електронні докази також можна класифікувати відповідно до методу, встановленого Міністерством юстиції США у 2002 році: однією з таких класифікацій є записи, створені за допомогою комп'ютерного програмного забезпечення, відомі як вихідні дані, такі, наприклад, як файли журналів, банкоматів та записи мобільних телефонів. Цю класифікацію можна визначити як класифікацію за методом створення даних. Одним з різновидів способів класифікації цих доказів є записи, збережені шляхом підключення даних, частина яких була створена комп'ютерними програмами та програмним забезпеченням. Сюди входять цінні папери, які містять дані, оброблені розрахунками Excel. Іншою класифікацією будуть записи, які зберігаються на комп'ютері, наприклад письмові документи, що зберігаються як файли обробки текстів. Сюди також входять повідомлення в чат та збережені електронні листи [66].

Третій спосіб класифікації електронних доказів – відповідно до мети, для якої вони створені (класифікація, яку можна визначити як класифікацію за призначенням). Відповідно до цього стандарту електронні докази поділяються на дві категорії. Перший – це докази, які можуть бути засобом доказування [153]. Сюди входять записи, створені автоматично, наприклад, рахунки за телефон і комп'ютерні записи, також включаються записи, частина яких була збережена в пристрої та оброблена програмним забезпеченням. Другий – докази, що не можуть бути використані як засіб доказування [67].

Для правозастосування в США, електронні докази мають характеристики, які відрізняють їх від інших традиційних доказів, серед яких найбільш помітною є їх науковість [82, с.4]. Науковість є результатом практичних експериментів із застосуванням наукового методу. Він використовується для надання достовірних даних і фактів, які були представлені для доведення або спростування фактів, і для цього потрібно використовувати високоякісні наукові дані та дані технічних фахівців, щоб переконатися, що докази достовірні [177]. Отже, те, що стосується наукових доказів, стосується й електронних доказів. Кожен вид доказів піддається перевірці на його достовірність. Електронні докази, представлені в судах, мають ґрунтуватися на науковій логіці, і їхня обґрунтованість не повинна бути під сумнівом [144].

Використання інформаційних систем залишає докази, які включають дані, надіслані чи отримані, а також кожне повідомлення, яке здійснюється мережею зв'язку. Дані на комп'ютері перекладаються системою за допомогою двох чисел, нуля та одиниці [184]. Ці дані також можуть бути доступні як цифрові докази.

Цифрові докази різноманітні та швидко вдосконалюються. Електронні докази відрізняються за формою та типом і можуть включати вихідні дані, системи моніторингу в мережах і серверах, або електронні документи та цифрові підписи, або аудіовізуальні записи чи вкладення, що зберігаються в

електронній пошті. Проте зараз розвиток кількох типів цифрових доказів характерний для віртуального світу. І це різноманіття спонукало законодавців до розробки законопроектів, щоб врахувати різні форми комп'ютерного виводу, включаючи електронні докази, проте результатів поки немає.

Щоб визначити значення «електронних доказів» саме в межах цивільного процесуального права США, необхідно, насамперед, звернутися до законодавства цієї країни. Водночас слід зазначити, що джерела писаного американського права поділяються на Конституцію США з відповідними поправками, статuti, міжнародні договори, правила судочинства, а також норми, правила та рішення адміністративних відомств. З усіх перерахованих видів федеральних нормативних актів для американського цивільного процесуального права особливе значення мають правила судочинства, розробка та прийняття яких відбувалися за активної участі представників судової влади, зокрема, Верховного Суду США.

Так, Федеральні правила про докази (Federal Rules of Evidence) [125], прийняті в 1975 році, вважаються серед дослідників основною кодифікацією доказового права США [200]. Таким чином, для отримання характеристики «електронних доказів» як правового явища необхідно звернути увагу, насамперед, на зазначений нормативно-правовий акт.

Федеральні правила про докази починаються з правила 101 параграфу I, яке містить визначення основних понять, що застосовуються у цьому акті. Пункт "b" цього правила встановлює, що у випадку, коли в тексті Федеральних правил про докази йдеться про письмові матеріали будь-якого виду, то мають на увазі також інформацію, що зберігається в електронній формі.

Крім цього, пункт "a" правила 1001 параграфу X Федеральних правил про докази вказує, що письмовий матеріал складається з букв, слів, цифр або інших аналогічних символів, зафіксованих у будь-якій формі. Практично аналогічне уточнення зроблено у відповідних пунктах "b" та "c" для таких

груп доказів, як записи та фотографії. Таким чином, словосполучення "інших аналогічних символів, зафіксованих у будь-якій формі" ("equivalent set down in any form"), з урахуванням положень пункту "b" правила 101 параграфу I розглянутого акта, передбачає можливість використання цифрової інформації як однієї з груп доказів, а саме: у вигляді письмових матеріалів, записів та фотографій, тобто тих засобів доведення, яким і присвячений параграф X Федеральних правил про докази.

Крім того, пункт "d" правила 1001 вказаного акта, встановлюючи критерії розмежування оригіналу документа від його копії, містить положення, спрямоване безпосередньо на регулювання діяльності з використання комп'ютерної інформації у процесі. Так, стосовно письмових матеріалів, записів і фотографій, то під оригіналом розуміється сам цей матеріал, запис або фотографія або їх аналог, що має те саме значення для особи, яка його виробила або випустила, що й оригінал. У той же час для інформації, що зберігається в електронній формі, розмежування копії та оригіналу побудовано на іншій підставі - у цьому випадку оригіналом визнається будь-який аналог документа, візуально доступний для читання, роздрукований на принтері або іншому вивідному пристрої, за умови, що останній здатен адекватно відобразити інформацію.

Федеральні правила про докази не містять інших положень, у яких прямо згадувалися б «електронні докази». Тим не менш, наведених вище норм достатньо, щоб зробити певні висновки.

По-перше, Федеральні правила про докази не містять поняття «електронного доказу», а оперують іншим терміном – «інформація, що зберігається в електронній формі» («electronically stored information»). По-друге, спеціальне правило про електронну інформацію міститься в параграфі, присвяченому звичайним групам доказів. По-третє, свідчення про те, що матеріали, записи й фотографії можуть зберігатися в будь-якій формі, є додатковою підставою припускати, що комп'ютерна інформація асоціюється

розробниками Федеральних правил про докази скоріш із різновидом традиційних видів доказів, а не з якимось особливим правовим явищем.

З іншого боку, американський законодавець все ж таки відступив від позиції рівності всіх груп доказів, встановивши спеціальні критерії відмежування оригіналу електронної інформації від її копії, чим, насправді, визнав певну специфіку цифрової інформації як доказу.

Сторона в судовому процесі США може забажати представити кілька типів електронних доказів під час судового розгляду, включаючи електронну пошту, текстові повідомлення; дані, що зберігаються в цифровому вигляді; цифрові фотографії; та інформацію в соціальних мережах. У цих сценаріях буде застосовуватися кілька правил подання доказів. Однак для прийняття електронних доказів потрібно подолати низку умов, передбачених Федеральними правилами про докази.

Першою умовою, яку необхідно подолати будь-якому запропонованому доказу, є аутентифікація. Згідно з Федеральними правилами про докази, «щоб задовольнити вимогу аутентифікації або ідентифікації предмета (доказу), ініціатор повинен надати докази, достатні для підтвердження висновку, що цей предмет є тим, яким він стверджується» (правило 901).

Аутентифікація цифрових доказів, як і паперових, «потребує доказів, достатніх для підтвердження такого висновку. Якщо суддя вирішить, що їх достатньо для присяжних, щоб зробити висновок, що докази є достовірними, тоді суддя вважатиме докази допустимими. Насправді рішення про достовірність доказів залишається на розсуд присяжних, які й вирішуватимуть цінність, яка надається певним доказам.

Аутентифікація цифрових доказів створює унікальні проблеми. З паперовими записами можна вносити зміни, легко впізнати, а автора чи зберігача ідентифікувати за підписом або стилем письма. У контексті зміни електронної інформації може бути важко або неможливо виявити автора й тому творця може бути неможливо розпізнати.

Як і паперові, електронні записи можуть бути засвідчені прямими або непрямыми доказами. Творець, наприклад, електронної таблиці Excel може забезпечити пряме свідчення авторства. Проблема - це легкість, з якою цифрова інформація може бути змінена, знищена або виготовлена.

Це навіть може бути досягнуто навмисно або випадково початківцем.

Реальність така, що доводиться електронні докази перевіряти цифровими експертами-криміналістами із знаннями, навичками та досвідом використання і застосовувати комплексних методів і засобів інформатики та інформаційної безпеки. Цифрові криміналісти використовують свої навички та інструменти, щоб отримати непрямі докази про цілісність і достовірність таких електронних доказів.

Електронні докази можуть бути перевірені кількома способами, найпоширенішим з яких є надання свідку особистих відомостей про інформацію – варіант, який відповідає вимогам правила для всіх типів електронних доказів. Якщо такого свідка немає, інші способи автентифікації включають:

- свідчення експерта або порівняння з автентичними прикладами [901(b)(3)];
- публічні записи [901(b)(7)];
- система або процес, що здатний забезпечити надійний результат [901(b)(9)];
- офіційні публікації [902(5)];
- засвідчена копія ділових записів, наприклад, міжофісних систем обміну миттєвими повідомленнями або Outlook [902(11)];
- сертифіковані записи, створені електронною системою [902(13)];
- сертифіковані дані, скопійовані з електронного пристрою, носія даних або файлу [902(14)].

Наступні умови прийнятності електронних доказів для використання в судовому засіданні містяться у правилах 401 та 402 Федеральних правил про докази, обидва з яких вимагають, щоб докази були релевантними

справі. Правило 401 забезпечує перевірку відповідних доказів («докази є релевантними, якщо: (а) вони надають будь-яку можливість зробити факт більш або менш вірогідним, ніж це було б без доказів; і (b) факт має значення при вирішенні позову») і правило 402, в якому зазначено, що «відповідні докази є прийнятними», якщо вони не визнані неприйнятними відповідно до Конституції Сполучених Штатів, федерального закону, інших федеральних правил доказів або правил встановлених Верховним судом США.

Проте іноді суди відмовляють у допуску відповідних електронних доказів. Одна з основних норм, що містять підстави для цього, – правило 403, яке забороняє введення відповідних доказів, «якщо їх доказова цінність загрожує небезпекою ... несправедливого упередження, плутання питань, введення в оману присяжних, невинуватеної затримки, витрачання часу або непотрібного подання доказів». Щоб сторона або суддя визначили, чи є запропоновані електронні докази доречними та прийнятними відповідно до правил 401, 402, 403 Федеральних правил про докази, вони повинні провести аналіз за трьома критеріями:

По-перше, чи мають докази тенденцію зробити факт, що має значення для позовів, які розглядаються, більш чи менш вірогідним, ніж якби докази не були прийняті?

По-друге, чи вимагають конституція, федеральний закон чи інші правила щодо доказів виключення запропонованих доказів?

По-третє, чи переважає доказова цінність доказу будь-які негативні чи шкідливі наслідки подання цих доказів, перераховані у правилі 403? Якщо ні, докази мають бути виключені згідно з правилом 403, навіть якщо вони мають значення відповідно до правил 401 і 402 Федеральних правил про докази.

Ще одним важливим доказовим правилом є «правило найкращих доказів». Є багато юристів, які з подивом дізнаються, що друкована версія текстової обробки електронного документа, ймовірно, вважатиметься непринятною відповідно до цього правила найкращих доказів, що буде оскаржено через наявність оригінального цифрового документа. Правило

найкращого доказу в сукупності правил від 1001 до 1008 покликане усунути ризик того, що паперові копії електронних доказів сфальшовані, вимагаючи запропонувати оригінал, якщо не мають місце певні винятки.

Важлива проблема використання в судовому доказуванні паперових копій цифрових документів полягає в тому, що паперова копія повною мірою не відповідає оригінальній цифровій версії, оскільки цифровий документ містить метадані. Метадані – це вбудована інформація, що зберігається в електронно створених матеріалах, але невидима при друкуванні цифрового документа. Зазвичай метадані навіть не відображаються під час перегляду цифрового документа на монітор комп'ютера за допомогою прикладної програми. Наприклад, обробка текстів документа автоматично створює метадані, які описують документ, його автора, дату створення і дати внесення змін, якщо такі були. Що стосується електронної пошти, метадані підкажуть хто копіював лист або коли його прочитали, тоді як паперова роздруковка не виявить таких джерел інформації. У деяких випадках, метадані можуть бути надзвичайно актуальними. В інших вони можуть не мати ніякої цінності, а його паперовий аналог матиме достатньо даних.

Наступна проблема використання в процесі судового доказування електронних доказів – це віднесення їх до так званих «*hearsay evidence*», найближчим аналогом яких у нашій правовій доктрині є похідні докази. Правила 801-803 Федеральних правил про докази пояснюють, що є «*hearsay*», а що ні. Щоб визначити, чи можна включити докази, які підлягають прийняттю, як чутки, сторона або суд повинні відповісти на такі запитання:

- чи є докази заявою? Висловлювання можуть бути письмовими, усними або невербальними, асертивними діями, такими як кивання або похитування головою декларанта;
- чи заява зроблена людиною (тобто її створила не машина);
- чи підтверджується твердження, запропоноване для визначення істинності справи?

Поширені винятки для електронних доказів включають:

- теперішнє смислове враження ([803(1)], приклади: публікація в соціальних мережах, текстове або миттєве повідомлення, електронна пошта тощо);
- схвильоване висловлювання ([803(2)], приклади: публікація в соціальних мережах, текстове або миттєве повідомлення, електронна пошта тощо);
- ділові документи ([803(6)], приклади: електронні листи, міжофісний обмін миттєвими повідомленнями, профіль робочого вебсайту тощо);
- загальнодоступні записи або звіти ([803(8)], приклади: поточні загальнодоступні вебсайти, включаючи Facebook, Instagram тощо); і
- свідчення репутації особи ([803(21)], приклад: дописи людей у спільноті у Facebook, що обговорюють репутацію людини).

Нарешті, залежно від того, який тип електронних доказів пропонується, може бути задіяне правило оригіналу. Відповіді на наступні запитання визначають, чи застосовується це правило до доказів, запропонованих стороною:

1. Чи є доказ:

- а) письмовим (що складається з букв, слів, цифр тощо, «записано в довільній формі»);
- б) записом (що складається з букв, слів, цифр тощо «будь-яким способом»); або
- с) фотографією (що складається із «зображення», яке «зберігається в будь-якій формі»)?

2. Якщо так, то чи є докази:

- а) оригіналом написання або запису, тобто чи має оригінал такий самий ефект від особи, яка його виконала або випустила; зокрема, для електронних доказів «оригінал означає будь-яку роздруківку – або інший результат, який можна наочно сприймати – якщо він точно відображає інформацію; або
- б) Оригінальна фотографія?

Якщо докази є не оригіналом, а дублікатом («аналогом, отриманим за допомогою механічного, фотографічного, хімічного, електронного чи іншого еквівалентного процесу чи техніки, що точно відтворює оригінал»), тоді докази не відповідають умові «оригіналу», встановленої правилом 1002 Федеральних правил про докази. Однак дублікат є прийнятним у тій же мірі, що й оригінал, якщо не виникає сумнівів у його відповідності оригіналу та обставини не свідчать про несправедливість використання дублікату (правило 1003).

Крім того, свідки з особистими знаннями, які можуть перевірити зміст письма, запису чи фотографії, є найкращим інструментом для виключення вимоги правила 1002 Федеральних правил про докази. Якщо свідок, який володіє знаннями, перевіряє і підтверджує зміст дублікату, надавачу доказів не потрібно надавати оригінал. Якщо достовірність дублікату або існування оригіналу піддається сумніву, присяжні повинні прийняти таке рішення на основі інформації, наданої під час судового розгляду.

Знання та розуміння цих правил допомагає адвокатам та їхнім клієнтам подати необхідні докази під час судового розгляду під час запиту та отримання електронної інформації на стадії відкриття судового процесу.

Більш опрацьований підхід до проблеми «електронних доказів» бачимо у Федеральних правилах цивільного процесу (Federal Rules of Civil Procedure) [124].

Правила визнають важливість електронної інформації. Правила надають цифровим документам таку ж вагу та статус, що й іншим доказам. Ці норми підкреслюють фундаментальне зрушення сучасного судового процесу на шляху повноцінного включення електронної інформації в судовий процес.

Правило 26(a)(1)(B) пояснює, що інформація, яка зберігається в електронному вигляді, включається в число документів та речей, які повинні бути включені в обов'язкове первинне розкриття стороною. Якщо сторона може використовувати цифрові докази для підтвердження своїх претензій

або захисту, тоді сторона повинна розкрити копію цифрового документа. Щоб виконати цей обов'язок, адвокату необхідно зустрітися з клієнтом за участі спеціалістів з інформаційних технологій для складення необхідної інформації для включення до первинного розкриття.

Правило 26(b)(2)(B) вимагає створення відповідної електронної інформації, яка є «розумно доступною». Ця норма визначає, що певні форми зберігання інформації в електронному вигляді є обтяжливими й дорогими. Якщо сторона заперечує на підставі невиправданого навантаження або витрат на виготовлення інформації, яка не є такою легкодоступною, сторона, яка заперечує, повинна довести це навантаження.

Щодо правила 34, то спочатку воно зосереджувалося лише на «документах» і «речах», але пізніше термін «документи» був змінений, щоб включити «компіляції даних». Протягом багатьох років суди тлумачили термін «документи», включаючи інформацію, збережену в електронному вигляді, яка може зберігатися в різних формах. Чинне правило 34(a) визначає «документи» як «збережену в електронному вигляді інформацію», і ця фраза навіть включена в назву. Також існує норма, що підтверджує подання електронних даних нарівні з поданням паперових документів, тому одержувачі запитів на виготовлення «документів» тепер мають чіткий обов'язок прийняти запит і надати не тільки паперові документи, а й всю відповідну інформацію, що зберігається в електронному вигляді, незалежно від носія, на якому вона зберігається.

Поправка до правила 34(a) роз'яснює, що сторони можуть вимагати можливості «перевірити» або «зразки» відповідних документів або інших матеріальних речей, включаючи інформацію, що зберігається в електронному вигляді.

Правило 34(b) також було змінено, щоб дозволити запитуючій стороні «вказати форму або форми, в яких має бути створена інформація, що зберігається в електронному вигляді». Якщо запитувач не вказує форму, респондент може вказати форму або форми, в яких вона буде

виготовлена. Незалежно від форми, в якій створюється цифрова інформація, правило 34(a)(1) вимагає, щоб вона була «перекладена, якщо необхідно, відповідачем у розумно придатну для використання форму».

Якщо запитуюча сторона вказує форму, проти якої відповідач заперечує, а сторони не можуть досягти згоди, респондент «повинен надати інформацію у формі чи формах, в яких вона є і зазвичай підтримується або у формі чи формах, які є розумно придатними для використання». Передача інформації в цифровому вигляді, тобто в тому вигляді, в якому вона зазвичай зберігається, означає передачу інформації в її рідному форматі, як вона є, і зберігається на пристрої, що може означати включення метаданих. Як наслідок, поширена практика перетворення всіх документів, отриманих із цифрового пристрою, у формат TIF буде недостатнім, якщо це не погоджено або не наказано судом.

Суд, у свою чергу, може прийняти рішення про форму інформації незалежно від запропонованих сторонами.

Ще одним достатньо цікавим питанням, що регулюється у Федеральних правилах про докази є збереження електронних доказів. Протягом століть адвокати та їхні клієнти мали юридичний обов'язок вживати розумних заходів для збереження потенційних доказів [74]. Знищення - це навмисне або необережне знищення або зміна доказів або небереження майна для використання в якості доказів у певному або в майбутньому судовому процесі [145].

Цифрова інформація має декілька відмінностей, стосовно збереження, на відміну від паперової чи матеріальної. «Невидимі» цифрові дані відрізняються, насамперед, через великий обсяг. Це дешево й легко зберігати гору магнітних даних на кількох жорстких дисках комп'ютера, сервері чи резервній копії. Одне електронне повідомлення створює кілька копій: одну в папці відправника; одну на жорсткому диску відправника; одну на сервері електронної пошти; одну на жорсткому диску одержувача. Цей цифровий слід дуже великий.

А друга відмінність полягає в тому, що незліченні невинні помилки можуть змінити або знищити архіви інформації, навіть якщо вони належним чином збережені від псування. Що ще гірше, суди швидко накладають санкції на тих, хто не виконує належним чином норм щодо зберігання або подання цифрових доказів.

Згідно з ретельним дослідженням усіх думок, санкції накладаються за неналежне збереження або надання цифрових доказів і залежать від двох факторів: ступеню винуватості та ступеню упередженості [204]. Чим вищий ступінь винуватості, тим менше доказів упередженості необхідно для виправдання санкцій і навпаки. Дослідження Г. Палмера також виявило, що санкції накладалися в 65% випадків, при чому на відповідачів накладалися в чотири рази частіше, ніж на позивачів. З випадків, коли були запроваджені санкції, 85% стосувалися одночасно незбереження доказів, псування та затримки подання, 35% - на упередження; і 9% через звичайну недбалість. Коли санкції призначалися, то у 60% вони включали присудження витрат з гонорару адвоката, 30% включали недопущення доказів; 23% передбачали негативні вказівки присяжних, а 28% – два або більше цих засобів [187].

Кілька сумнозвісних випадків наочно ілюструють небезпеку невдалого збереження і подання цифрових доказів. Одним із ранніх знакових випадків у виплаті є справа Zubulake проти UBS Warburg, LLC, яка породила численні опубліковані думки стосовно цього питання. Федеральний суд наклав санкції на UBS через багато причин, у тому числі, за неспроможність зберегти резервні копії, які містять дуже релевантні електронні листи та інші цифрові докази [236]. Одна санкція включала негативний висновок, в якому вказувалось, що UBS знищила відповідні докази, оскільки це могло зашкодити їх захисту. Суд присудив Зубулаке Стіну (торговець акціями) компенсувати 9 мільйонів доларів втраченої заробітної плати та 20 мільйонів доларів відшкодування збитків.

Обов'язок зберігання виникає, як тільки людина дізнається або повинна була знати, що матеріали мають відношення до розгляду позову або до

обґрунтовано очікуваного майбутнього судового процесу. У справі Zubulake суд постановив, що обов'язок зберігати виникла якомога раніше, коли менеджери UBS почали боятися, що Зубулаке може подати позов.

В іншій відомій справі, пов'язаній із санкціями, Prudential Insurance було оштрафовано на 1 мільйон доларів США, тому що виявлено необережне знищення документів [154]. Усі працівники були повідомлені про судовий процес, і Prudential було наказано оприлюднити політику збереження документів. Це, мабуть, найбільш сумнозвісна справа про санкції, пов'язані з виявленням даних, що призвела до вироку присяжних у розмірі 1,4 мільярда доларів.

Слід сказати, що Федеральні правила цивільного процесу, безсумнівно, призводять до більш остаточних рішень щодо збору та дослідження електронних доказів.

Крім законодавства, юридична доктрина США також активно досліджує «електронні докази» як особливе правове явище. У той самий час, якщо вітчизняні дослідники, вирішуючи питання виділення комп'ютерної інформації як окремого виду доказів, спираються на технічні аспекти роботи цифрових пристроїв, їх західні колеги звертають більше уваги на юридично значимі особливості комп'ютерної інформації.

«Електронні докази» визначаються американськими правознавцями як відомості, що обробляються, зберігаються або передаються будь-яким штучним пристроєм, комп'ютером або комп'ютерною системою, та які представляють ту чи іншу обставину, що має значення для справи, як більш-менш ймовірну [116]

На підставі аналізу американської спеціальної літератури можна виділити велику кількість юридично значимих характеристик комп'ютерної інформації, проте, враховуючи специфіку цього дослідження, найбільш розумним видається зупинитися лише на деяких з них.

Однією з найважливіших властивостей електронних носіїв інформації є значний обсяг пам'яті [161]. Справа в тому, що цифровий пристрій, що

належить особі, може нести такий величезний масив інформації про його життя, який раніше міг би охопити велику кількість томів. Більше того, збережена на комп'ютері інформація може бути представлена не лише текстовими файлами, а й як відео-, аудіозаписи. Все це робить цифровий пристрій найбільш інформативним джерелом інформації про його власника.

Таким чином, потенціал цифрових пристроїв, що полягає в зберіганні величезних масивів різноманітних інформації, є юридично значущою властивістю «електронних доказів», оскільки вимагає аналізу в рамках законодавчої та правозастосовної практики.

Другою важливою властивістю «електронних доказів», що виділяються американськими правознавцями, є легкість копіювання відомостей, що містяться в них. Якість копіювання тут знаходиться на такому високому рівні, що єдина різниця між оригіналом документа та його копією може полягати лише в часі створення файлів.

Також важливими властивостями «електронних доказів», які часто згадуються в літературі, є неочевидність і відносність їхнього змісту.

Неочевидність змісту, передусім, обумовлена тим, що будь-які дані, записані за допомогою комп'ютера, частково є прихованими метаданими, тобто відомостями про характеристики об'єктів - носіїв інформації, сприяють ідентифікації, виявленні, оцінці та управлінню цими об'єктами. Такі метадані можуть містити інформацію про час створення файлу, його автора, час його останньої зміни, про місце, де він зберігався з моменту створення, спроби отримати до нього доступ і багато інших відомостей. Більшість звичайних користувачів не знають про існування цих даних, тому що для їх огляду необхідно мати певні навички або використовувати спеціальне програмне забезпечення, у той час як для фахівців дослідження такої інформації не становить жодної складності.

Неочевидність змісту проявляється також і в тому, що до моменту відкриття певного файлу не можна напевно судити про його зміст. Так, файли з розширенням, притаманним для фотографій, можуть містити текст,

який був сфотографований, відеопрогравачі можуть зберігати виключно звукові записи, а текстові файли включати малюнки тощо. Більш того, шляхом простої операції файли з одним розширенням можуть бути навмисне переведені в інше.

Відносність змісту електронних доказів передбачає, що навіть той обсяг інформації, який доступний для огляду звичайним користувачам, не завжди однаковий, тому що варіюється залежно від програмного забезпечення конкретного комп'ютера та його налаштувань. Відомо, наприклад, що текстовий файл може бути відкритий безліччю текстових редакторів, кожен із яких представить їх у різному вигляді. Так, один з редакторів може відобразити текст у вигляді певної структури, тоді як інший виведе на монітор лише сукупність сторінок, що послідовно йдуть один за одним. При цьому, навіть змінюючи основні параметри налаштувань такого класичного редактора як Microsoft Word, можна отримати різні інтерпретації одного й того ж файлу.

Ці, здавалося б, суто технічні особливості цифрової інформації, мають важливе значення для правозастосовної діяльності судів США. Справа в тому, що при відмежуванні приватних відомостей від публічних, юридична практика ґрунтується на такому стандарті, як «розумні очікування з приводу таємниці особистого життя», однак визначити такі очікування щодо інформації, яка частково прихована, частково невизначена за змістом, досить складно [96].

Нарешті, остання особливість комп'ютерної інформації в тому, що вона може зберігатися як у пам'яті самого пристрою, і бути отримана через інформаційно-телекомунікаційну мережу інтернет чи іншу комунікаційну систему. У зв'язку з цим, отримуючи доступ до комп'ютера, представник сторони звертається до джерел даних, які можуть зберігатися віддалено, у тому числі за межами державних кордонів США.

З урахуванням зазначених доктринальних напрацювань, під «електронним доказом» необхідно розуміти електронний носій інформації,

що містить відомості про значущі обставини в конкретній справі та має такі ознаки: а) потенційно значний обсяг пам'яті; б) простота передачі та копіювання відомостей з одного електронного носія інформації на інший; в) можливість віддаленого доступу до змісту електронного носія та інформаційно-телекомунікаційних систем (зокрема, до мережі інтернет); г) відносність та неочевидність змісту.

Підсумовуючи, необхідно зазначити, що зазначені властивості цифрових пристроїв, відзначені сучасними американськими вченими, дійсно претендують на роль відмінних рис «електронних доказів» саме як юридичного явища.

У підсумку необхідно зазначити, що термін «електронний доказ» («electronic evidence») у нормативно-правових актах США не використовується та більшою мірою розроблений правовою доктриною. Дійсно, представник вітчизняної правової науки, для якої характерний чіткий поділ доказів на види за критеріями, ймовірно, зверне увагу на відсутність у законі спеціального терміна для позначення того чи іншого поняття, що може призвести його до думки про відсутність у праві шуканого явища. Такі міркування, однак, не мають великого значення для американської правової системи, де ні у Федеральних правилах цивільного процесу, ні у Федеральних правилах про докази не закріплено і таке знайоме кожному вітчизняному юристу поняття як «речовий доказ».

Неувага законодавства США до правових понять є загальною особливістю для всіх представників англосаксонської правової сім'ї, яка, як було зазначено, більше схильна до вирішення практичних проблем, що виникають у юридичній діяльності.

Другим важливим моментом у вирішенні проблеми «електронних доказів» є вищезазначена процедура копіювання комп'ютерної інформації. В американському процесуальному законодавстві копіювання виступає в ролі процедури отримання доказів, що здійснюється з волі самої сторони.

Важливою відмінністю українського права від американського є також те, що останнє включає як джерело судовий прецедент, який істотно впливає на правове регулювання суспільних відносин у тій чи іншій сфері.

На відміну від нормативно-правових актів, що зберігають певну стабільність, судді набагато частіше у своїх рішеннях вказують на специфічні особливості «електронних доказів», необхідність встановлення нових юридичних стандартів при обробці комп'ютерної інформації. Приміром, розглядаючи справу "United States versus Adjani" (2006), суддя зазначив, що застосування положень Четвертої поправки Конституції США щодо пошуку інформації на комп'ютері є складним питанням, і суди, у міру розвитку інформаційних технологій, покликані аналізувати нові юридичні ситуації та виробляти нові правила поза положеннями Четвертої поправки Конституції США [116].

Зазначене твердження, з урахуванням випадків із судової практики, дозволяє з упевненістю заявити, що для прецедентного права США «електронні докази» є значущим правовим феноменом, а постійне оперування цифровими пристроями часто змушує суддів приділити особливу увагу та більш точно роз'яснити існуючі правові стандарти, що з часом веде до вироблення нових правил процесуальної діяльності.

Водночас наведені вище положення є достатніми для того, щоб розглядати «електронні докази» як важливу та невід'ємну складову інституту судового доказування в цивільному процесуальному праві США.

2.2. Консервативний підхід до електронних доказів у цивільному судочинстві Великобританії

Великобританія складається з чотирьох регіонів: Англія, Уельс, Північна Ірландія та Шотландія, кожен з яких має власну правову та судову систему. У роботі досліджується саме процесуальне право Англії та Уельсу,

що мають найбільш характерні ознаки серед законодавства інших суб'єктів, що входять до складу Великобританії.

Судова система Англії та Уельсу формувалася протягом століть. Досі збереглися й її архаїчні риси. Їхня судова система має низку особливостей, властивих тільки їй і не властивих іншим державам.

По-перше, в Англії та Уельсі фактично відсутня єдина судова система, хоча прагнення такої спостерігається.

По-друге, переважна більшість цивільних справ розглядається не в судах, а в досудових, альтернативних процедурах та установах, у тому числі за участю суддів.

По-третє, в Англії та Уельсі різні суди мають неоднакове організаційне становище та структуру. Над ними немає і ніколи не було єдиного центру, який би здійснював організаційне керівництво судами.

Судову систему Англії та Уельсу утворюють суди загальної юрисдикції: 1) нижчі суди (магістратські суди (Magistrates Courts), суди графств (County Courts), суд у справах сім'ї (Family Court)); 2) вищі суди Англії та Уельсу: Апеляційний суд (Court of Appeal), Високий суд (High Court of Justice) та Суд Корони (Crown Court). 3) на чолі судової системи Великобританії став Верховний Суд Сполученого Королівства (Supreme Court of the United Kingdom). Окрім цього, функціонують інші суди чи суди спеціальної юрисдикції. До них відносяться: 1) Апеляційний суд з трудових спорів; 2) Коронерські суди. Значну роль грають Судові трибунали: 1) Суд із розгляду трудових спорів; 2) адміністративні трибунали (у справах про оренду, у справах землеволодіння, у спорах про соціальне страхування, промислові трибунали); 3) внутрішні суди (дисциплінарні суди). Функціонують також третейські суди (арбітражі), до яких належать: 1) арбітраж щодо визначення якості товарів та послуг; 2) арбітраж за технічними нормами; 3) змішаний арбітраж.

Магістратські суди відносяться до судів Англії та Уельсу, що стоять найнижче. Вони виникли у XIV ст. і у своєму розвитку зазнали низки змін.

Діяльність сучасного магістратського суду регламентується Законом про магістратні суди 1980 р. Здебільшого вони розглядають кримінальні справи, але їм підсудні деякі цивільні справи.

Суди графств створено у 1846 р. Усього їх налічується близько 270. Вони мають лише цивільно-правову юрисдикцію. На них припадає основне навантаження щодо розгляду цивільних справ. Щороку судами графств розглядається 1,5 млн справ. Повна ж судова процедура проходить лише по 5% справ, у решті випадків справи припиняються за примиренням сторін. Діяльність судів графств регламентується Законом про суди графств 1984 року.

Суд у справах сім'ї був створений у квітні 2014 року, коли відповідні розділи Закону про суди та злочини 2013 року набули чинності, і вперше за всю історію судової системи Англії та Уельсу в одному суді були зосереджені судді всіх рівнів сімейної судової системи – маїстрати, судді районних та окружних судів, а також судді Відділення у справах сім'ї Верховного суду. Сімейний суд має національну юрисдикцію. Однією з переваг нового Суду є скорочення зайвих витрат часу та ресурсів на передачу справ між різними судами, у чому полягав основний недолік попередньої структури.

Щодо Вищих судів Англії та Уельсу, то до них відносяться три судові органи: 1) Апеляційний суд; 2) Високий суд; 3) Суд Корони.

Апеляційний суд – основна ланка, де оскаржуються рішення всіх судів, що стоять нижче. Складається із 28 суддів. З 1966 р. організаційно поділено на два відділення: а) у цивільних справах; б) у кримінальних справах. Високий суд об'єднує три різні відділення суду: а) Суд королівської лави (Queen's Bench Division); б) Канцлерське відділення Високого суду (Chancery Division); в) відділення Високого суду із сімейних справ (Family Division). Це не самостійні суди, а структурні підрозділи Високого суду. І третій Вищий суд Англії та Уельсу - Суд Корони розглядає кримінальні справи. Створено відповідно до Закону про суди 1971 р., що зараз має у складі і також

Центральний кримінальний суд. У ньому розглядаються найскладніші кримінальні провадження.

Крім судів, що входять до судової системи Англії та Уельсу, є ще ціла низка інших судів – судів спеціальної юрисдикції. Вони призначені до розгляду певних категорій справ. Апеляційний суд з трудових спорів діє відповідно до Правил Апеляційного трибуналу з трудових спорів 1980 р. Коронерські суди – особливий орган, до функцій якого входить проведення офіційної попередньої перевірки фактів та випадків настання непротиправної, але й неприродної смерті людини. Суд у справах про заборонений торговельний обіг організований у 1956 р. для розгляду справ про порушення антимонопольного законодавства у сфері торгівлі. Військові суди призначені для вирішення справ про правопорушення, скоєні військовослужбовцями. Судові трибунали є органами адміністративної чи дисциплінарної юстиції, вони запроваджуються статутами парламенту або іншими актами делегованого законодавства для вирішення спорів між органами уряду та приватними особами.

Основними джерелами, що регулюють процес судового доказування в британських судах є:

1. Правила цивільного судочинства 1998р. (Civil Procedure Rules) [99].
2. Закон про докази в цивільному судочинстві 1968 (Civil Evidence Act 1968) [23].
3. Закон про докази в цивільному судочинстві 1972 р. (Civil Evidence Act 1972) [24].
4. Закон про докази в цивільному судочинстві 1995 р. (Civil Evidence Act 1995) [25].
5. Закон про докази (процедури в інших юрисдикціях) 1975 р. (Evidence (Proceedings in other jurisdictions) Act 1975) [22].

В Англії інститут доказування охоплює велику кількість норм, багато з яких формувалися практикою за довгі роки еволюційного розвитку.

Положення доказового права роблять вирішальний вплив на всі процесуальні форми й цим сприяють досягненню основних цілей правосуддя.

У сучасній юридичній літературі нерідко можна знайти критичні зауваження на адресу англійської системи доказів. Ці зауваження супроводжуються вимогами удосконалити інститут доказів чи його окремі частини [160].

В англійській юриспруденції можна знайти різні підходи до визначення судових доказів. Проблеми вивчення даного поняття зростають через багатозначне вживання таких термінів, як «evidence» і «proof». Терміном «доказ» (evidence) позначають факти чи засоби їх встановлення. «Докази - це всі факти, документи та показання, а також інші законні засоби, які можуть бути використані для встановлення спірного факту» [160]. Головними різновидами судових доказів є свідчення, відомості з похідних джерел, документи, речі та факти, які суд приймає для з'ясування головних спірних обставин у цій справі.

З точки зору суто практичної, доказом рекомендується вважати «...матеріал, який учасник справи бажає представити суду в надії, що це спонукає суд дійти бажаного висновку з питання факту» [160].

Термін «proof» також неоднозначний. Ймовірно, найпоширенішою є думка, що proof – це те, що веде до висновку про правдивість чи фальшивість тверджень про факти. Evidence є підставою proof. Якщо evidence заслуговує на довіру, воно може мати результатом proof [45].

Огляд дефініцій дає можливість зробити висновок, що термін «evidence» має ряд аспектів. Він використовується для позначення фактів, за допомогою яких шукають дорогу до головних фактів, усієї суми прийомів доказування, конкретних засобів доказування, а також свідчень. Під поняттям proof мається на увазі діяльність із доведення чи її результати.

Відповідно до вищевказаних нормативно-правових актів у англійському праві можна виділити три засоби доказування: показання свідків, письмові та речові докази.

Показання свідків широко використовуються в цивільному процесі Англії як засіб доказування (*means of proof*). І якщо континентальні правові системи вважають пояснення сторін та висновки експертів особливими видами доказів, то англійська юриспруденція традиційно відносить їх до показань свідків, щоправда, вони мають ряд специфічних рис.

Головні питання, що виникають у зв'язку з цим джерелом інформації, стосуються здатності людей бути свідками (*competence*), можливістю їхнього примусового виклику до суду (*compellability*) та допустимістю відмови розкривати деякі відомості (*privilege*).

В англійському праві склалася загальна норма, яка встановлює залежність компетентності людини свідчити в цивільних справах лише з його інтелектуальних і фізичних характеристик. Такі обмеження поширюються, звісно ж, на дітей і психічно хворих. Дорослі розсудливі люди, безумовно, можуть давати свідчення.

Заходами, які мають гарантувати достовірність інформації, є присяга або обіцянка свідка не брехати. Умисне порушення клятви чи обіцянки має однакові юридичні наслідки.

В англійській практиці свідків запрошують до суду учасники цивільно-правового конфлікту. Юридичні норми, що фіксують принцип змагальності в його англійській інтерпретації, цілком покладають обов'язок збирання доказів на зацікавлених осіб. Судді ініціативи щодо виклику свідків не виявляють, більше того, їм заборонено це робити, крім як за згодою або, принаймні, за відсутності прямих заперечень сторін. Суддя може лише наказати ще раз допитати вже раніше допитаного свідка.

Здавна існує два різновиди повідомлень, що надсилаються особі, яка має відвідати суд. Одна повістка називається *subpoena ad testificandum* – виклик для надання показань, інша – *subpoena duces tecum* ("принести з собою") – явка з поданням зазначених документів [160].

У суді свідок повинен відповідати на запитання, що ставляться учасниками справи й судом, та подавати наявні в нього документи або

предмети. Водночас, в англійському праві існують норми, що дозволяють свідку з власної ініціативи або з ініціативи зацікавленої сторони відмовитись дати певну інформацію. Йдеться про так звані приватні або особисті привілеї (private privilege).

Свідки також мають право на відшкодування витрат, які вони несуть через виклик для надання показань. Наукові свідки (експерти) отримують також винагороду за виконану ними роботу. Витрати оплачують сторони. Ці питання регламентуються численними підзаконними актами.

Також англійською юриспруденцією давно встановлено загальне правило: свідки повинні розповідати лише про факти, які вони сприймали, але не про свої думки, висновки або судження щодо фактів (opinion).

Автори багатьох теоретичних праць, навіть спеціально присвячених доказовому праву Англії, уникають давати хоча б найпримітивніше визначення поняття письмових доказів. Зазвичай цей термін (documentary evidence) вживається як щось цілком очевидне. Але набагато частіше як синонім використовується термін «документи» (documents), яке за змістом може бути різним залежно від контексту або намірів того, хто таке слово застосував.

Наприклад, ст. 10 (1) закону 1968 р. роз'яснює, що в рамках цього статуту термін «документ», крім письмових актів, охоплює також: а) карти, плани, графіки чи креслення; б) фотографії; в) диски, стрічки, звукові доріжки, інші пристрої, за допомогою яких звуки зафіксовані й можуть бути відтворені; г) фільми, негативи, що закріпили зорові образи та здатні їх відтворювати. Копіями документів за ст. 10 (2) називаються також копії магнітофонних записів, репродукції зображень і т.д.

Ці норми свідчать про надзвичайно широке тлумачення поняття «документ», що безумовно включає також якусь частину речових доказів. Проте найбільше значення для цивільного судочинства мають письмові докази чи документи у вузькому, безпосередньому значенні цього терміну, тобто письмові акти. До цих актів учасники цивільно-правових спорів

вдаються мало не в кожній справі. Ними підтверджуються чи спростовуються факти укладання договорів, складання заповітів, їх умови, взаємини в галузях винахідництва, спадкування, деліктів та багато іншого. Від кількості та характеру документів залежить також, чи буде задоволено клопотання про розгляд справи за участю присяжних засідателів.

Речові докази (real evidence) становлять третій різновид засобів доказування, відомий англійському судочинству. Матеріальні об'єкти, які своєю наявністю, якостями, формою та іншими рисами підтверджують або спростовують якісь факти, що стосуються справи, фігурують у цивільних процесах.

Найчастіше використовуються різного роду фізичні об'єкти, що доставляють на засідання, де їх вивчає суд (exhibits). У цивільних справах це можуть бути зразки товарів, зіпсовані чи пошкоджені речі тощо.

Звичайним методом вивчення є візуальний огляд, хоча іноді набувають значення звукових сприйняття (якість музичного інструменту) або смакових відчуттів (вміст пляшки). Якщо необхідно збереження таємниці, то предмети досліджуються на закритому засіданні.

До речових доказів також відносять зовнішні риси людей (appearance of persons). Отримані поранення, каліцтво, спотворення можуть свідчити про заподіяння шкоди та враховуватися при обчисленні розміру компенсації. Допустимо також наочно оцінювати загальний стан здоров'я людини, старість або, навпаки, молодий вигляд. Навіть портретна подібність між дитиною та її передбачуваним батьком може мати доказове значення у справах про встановлення батьківства.

Як можна було помітити, за цивільним процесуальним законодавством Англії та Уельсу так само як і в законодавстві США не виділяється такого окремого виду доказів як електронні докази. У Правилах цивільного судочинства йдеться лише про процедури та правила подання електронних документів, як і в цивільному процесуальному законодавстві США.

Правила подання регулюється двома окремими порядками: 1) відповідно до Практичної вказівки 51U [192], яка діє в Судах у справах бізнесу та спорах щодо власності; 2) згідно з частиною 31 Правил цивільного судочинства (далі – ПЦС), що діють в інших судах судової системи Англії.

Здійснювана в даний час модернізація подання документів в Англії (2019 – 2021 рр.; ПВ 51U) має дві мети: по-перше, зберегти роль англійських судів на світовій арені, сприяти продовженню залучення іноземних інвесторів в економіку (що призведе не тільки до самоокупності судової системи, а й зробить її позитивною статтею державного бюджету), по-друге, повернути реальний доступ до правосуддя для фізичних осіб, а також невеликих та середніх компаній.

Подання електронних документів є досить новою сферою, яка поряд із ПЦС регулюється ПВ 31 Б – Подання електронних документів.

Фактори, які необхідно оцінювати при визначенні обґрунтованості пошуку електронних документів, зазначені в ПЦС 31.7(2) та ПВ 31 (параграф 21):

- характер та складність справ;
- значення документа, який ймовірно буде знайдено під час пошуку;
- кількість документів;
- доступність документів або інформації з інших ресурсів;
- простота та вартість пошуку.

Останній фактор є центральним, суд оцінюватиме доказову корисність та вартість (витрати). Саме з цією метою ПВ 31 параграф 21(3) розкриває цей критерій:

- доступність електронного документа на комп'ютерних пристроях, серверах, резервному копіюванні та інших електронних пристроях, які можуть містити даний документ, враховуючи необхідне програмне забезпечення та (або) засоби необхідні для отримання, вилучення даного документа;

- місцезнаходження електронного документа, інформації, комп'ютера, сервера, резервної системи та інших електронних пристроїв;
- ймовірність виявлення даної інформації;
- вартість поновлення електронного документа;
- вартість розкриття та забезпечення проведення інспекції електронного документа;
- ймовірність того, що електронний документ буде змінено під час його відновлення, розкриття та інспекції.

Згідно п. 5 ПВ 31В «Електронний документ» означає будь-який документ, що зберігається в електронній формі: електронна пошта та інші електронні засоби зв'язку, такі як текстові повідомлення і голосова пошта, текстові документи і бази даних, а також документи, що зберігаються на портативних пристроях, таких як карти пам'яті і мобільні телефони. На додаток до документів, які легко доступні з комп'ютерних систем та інших електронних пристроїв і носіїв, включаються документи, які зберігаються на серверах і системах резервного копіювання, і документи, які були видалені. Він також включає метадані та інші вбудовані дані, які зазвичай не видно на екрані або на роздруківці. Розрізняються поняття «Електронне зображення» паперового документа та «Власне електронний документ» - електронний документ, що зберігається у вихідній формі, в якій він був створений за допомогою комп'ютерної програми [191].

Сторони та їх законні представники повинні враховувати такі загальні принципи щодо електронних документів:

- (1) електронними документами слід керувати ефективно, щоб мінімізувати понесені витрати;
- (2) слід використовувати технології, щоб гарантувати, що діяльність з управління документами здійснюється ефективно та дієво;
- (3) подання інформації має здійснюватися таким чином, щоб забезпечити досягнення основної мети;

(4) електронні документи, як правило, повинні бути доступні для перевірки у формі, що дозволяє стороні, яка отримує документи, мати таку саму можливість доступу, пошуку, перегляду та відображення документів, що й сторона, яка розкриває інформацію.

Перевірка кожного документа може бути дуже дорогою та тривалою за часом, тому дозволено проводити пошук за ключовими словами, або використовуючи автоматичні методи пошуку інформації (ПВ 31 Б параграф 25). При пошуку сторони повинні використовувати програмне забезпечення, яке здатне скоротити час даного пошуку.

У справі *West African Gas Pipeline company ltd v Willbros Global holdings Inc* було зазначено три основні проблеми. По-перше, позивач не виконав обов'язок щодо уникнення подвоєння документів, що призвело до того, що копії документів було розглянуто велику кількість разів. По-друге, позивач не підготував усі електронні документи, що призвело до неповноти інформації. По-третє, суд дійшов висновку, що було підготовлено неправильний огляд початкових документів, що призвело до помилок [229].

Принцип ранньої взаємодії між юристами з розкриття електронних доказів у ПВ 31 Б відображено в Декларації про взаємодію, прийнятій Конференцією Седону (*the Sedona Conference Cooperation Proclamation*) [218]. Наслідки відсутності взаємодії та кооперації проілюстровані у справі *Digicel ltd v Cable & Wireless plc* [110].

У розкритті електронних доказів існують такі проблеми:

- відсутність достатніх вказівок у тому, як норми ПЦС про розкриття доказів застосовуються до електронних доказів;
- відсутність ясності між «розумним» та «пропорційним» пошуком електронних документів;
- складність та витратність пошуку електронних документів;
- відсутність взаємодії між сторонами при здійсненні розкриття електронних доказів, що призводить до різного обсягу пошуку документів;

- відсутність єдиного розуміння щодо обов'язку сторони зберігати електронну інформацію;
- різні способи подання сторонами електронних документів;
- побоювання сторін, що запити про розкриття електронних доказів є знаряддям боротьби під час розгляду справи;
- небезпека того, що витрати на пошук, збирання, перегляд, надання електронних документів будуть перевищувати суму позову [167].

Сторони повинні обговорювати один з одним, як вони зберігають електронні документи та здійснюють пошук електронних документів до першої конференції. Сторони можуть надавати одна одній інформацію про категорії електронних документів, що знаходяться під їх контролем, комп'ютерні системи, електронні пристрої, на яких може знаходитися інформація, що запам'ятовує пристрої, і політику зберігання документів (внутрішніх правил). Дані вказівки також встановлюють, які фактори мають бути враховані під час вирішення питання про розумний, обґрунтований пошук інформації. Вони передбачають можливість використання пошуку за ключовими словами або надання документів, що містяться на певних носіях.

При цьому законодавство Англії та Уельсу не містить вимоги в цивільному судочинстві (в тому числі сімейному та комерційному) використовувати якісь особливі шляхи отримання/вилучення електронних доказів (у нотаріуса, судового пристава, експерта чи ін.), наприклад, якщо сторона хоче подати докази із загальнодоступних вебсайтів в інтернеті.

Згідно Практичної вказівки 31В (п.28), якщо копії розкритих документів надаються у власному форматі, деякі метадані будуть розкриті з кожним документом. Сторона, яка запитує розкриття додаткових метаданих або судових копій зображень розкритих документів (наприклад, у зв'язку із спорами, що стосуються автентичності), повинна продемонструвати, що актуальність і значущість запитаних метаданих виправдовують витрати й тягар створення цих метаданих. За винятком випадків, коли існує домовленість або замовлено інше, електронні копії розкритих документів

повинні бути надані в їх власному форматі таким чином, щоб зберігалися метадані, асоційовані з датою створення кожного документа (п. 33). Сторона повинна надати всі доступні для пошуку версії електронних документів з функцією OCR (функцією розпізнавання за допомогою комп'ютера) разом з оригіналом (п. 34).

Електронні докази презумуються достовірними, якщо вони не оспорується. В Англії та Уельсі існує така презумпція, запроваджена Юридичною комісією, але це тема критики в професійних колах. Загалом існує два типи доказів: прямі та непрямі. Існування фізичного об'єкта є прямим доказом; непрямі докази охоплюють факти, які можна зробити з прямих доказів. Існує також юридичне визначення «real evidence», отриманих без втручання людини. Електронні докази підпадають під усі вищезазначені класифікації. Загальні правила щодо доказів полягають у тому, що суддя визнає майже будь-який доказ, і сторони повинні аргументувати вагу, яку він повинен надати йому [218].

Важливим правом сторони, яка не має доступу до електронних документів можливість звернутися до суду з проханням отримати копію електронних даних, що зберігаються на комп'ютері іншої сторони. Згідно Практичної вказівки 31В (п.15), якщо сторони вкажуть, що вони не змогли прийти до угоди щодо розкриття електронних документів і що досягнення угоди мало ймовірно, суд дасть письмові вказівки щодо розкриття інформації або призначить окреме слухання щодо розкриття інформації. [8, с. 10]

В Англії та Уельсі системи електронного подання судових документів впродовж останніх двадцяти років стрімко розвивались і не завжди мали позитивний результат, а часто кожен суб'єкт правосуддя користувався своєю програмою електронного документообігу, тому вважаємо за необхідне дослідити судову систему Англії і платформи електронного документообігу.

В українській процесуальній науці найбільш досконало та повно системи електронного документообігу було досліджено Н.Ю. Голубевою в своїй монографії [7].

Авторка зазначає, що на базі деяких судів діє Програма електронного документообігу (Electronic Working Pilot Scheme) з 2009 року (Адміралтейського (морського), Торгового судів, Лондонського промислового і торгового суду при Королівському суді (Commercial and London Mercantile Courts at the Royal Court of Justice (RCJ)). Подальший документообіг також відбувається в електронному вигляді. Крім вебсайту суду можна користуватися електронними скриньками, надсилати документи в електронному вигляді. Проте електронна форма подання позову до суду не є обов'язковою [137].

На сайті Верховного суду Об'єднаного Королівства можна ознайомитись із «Загальними принципами для електронного подання» (General guidelines for electronic bundles in The Supreme Court of the United Kingdom and Judicial Committee of the Privy Council) та правилами подання документів до Секретаріату Верховного Суду в електронному вигляді, – також за допомогою спеціальної електронної пошти.

У «The Chancery Division» Високого Суду (відділення Високого суду Великобританії, яке слухає в якості суду першої інстанції цивільні справи, пов'язані з управлінням майном, довірчою власністю тощо) діє «CE File» – це електронна система реєстрації та ведення справ, що працює з жовтня 2014 року, ТСС – з листопада 2014 року, в Адміралтейському і Комерційному суді – з липня 2015 року, і тепер вона також використовується для банкрутства компанії. Ця система дозволяє надсилати документи в суд в електронному вигляді та оплачувати судові збори онлайн [8].

Наразі CE-File використовується також у Senior Courts Costs Office (суд із визначення судових витрат, є частиною Високого Суду), а також для розгляду претензій і апеляцій у Відділення королівської лави Високого суду. Для юристів використання CE-File є обов'язковим у названих судах. Спроби подати документи поштою, факсом або електронною поштою не будуть задоволені.

Crown Court Digital Case System – платформа цифрової системи діловодства в Королівському Суді (Crown Court). Вона використовується для доступу, підготовки та подання інформації у справі. За її допомогою можна передавати документи не тільки в суд, а й іншій стороні, а також спільно працювати над документами [7].

Державною Радою з цивільного судочинства (Civil Justice Council) презентовано проєкт створення єдиної системи онлайн-судів. Основна думка розробників полягає в тому, що неперспективно використовувати інформаційні технології для підтримки існуючих процедур у судовій системі, тобто покращення того, що вже існує сьогодні. Це принципово не змінює основних процесів і процедур. Більш перспективним є використання нових способів відправлення правосуддя з підтримкою методів ODR. Йдеться не про власне ODR, а запозичення його ідей. Традиційний зал суду або кімната для засідання взагалі не має використовуватися, а використовується онлайн-сервіс [7].

Отже, можна зробити висновок, що в Англії та Уельсі не виділяється такого окремого виду доказів як електронні докази, а йдеться лише про процедури та правила подання електронних документів. «Електронний документ» визначається, як будь-який документ, що зберігається в електронній формі: електронна пошта та інші електронні засоби зв'язку, такі як текстові повідомлення і голосова пошта, текстові документи й бази даних, а також документи, що зберігаються на портативних пристроях, таких як карти пам'яті й мобільні телефони. На додаток до документів, які легко доступні з комп'ютерних систем та інших електронних пристроїв і носіїв, включаються документи, які зберігаються на серверах і системах резервного копіювання, і документи, які були видалені. Він також включає метадані та інші вбудовані дані, які зазвичай не видно на екрані або на роздруківці. Розрізняються поняття «Електронне зображення» паперового документа та «Власне електронний документ» - електронний документ, що зберігається у

вихідній формі, в якій він був створений за допомогою комп'ютерної програми.

РОЗДІЛ 3.

ЕЛЕКТРОННІ ДОКАЗИ В ЦИВІЛЬНОМУ СУДОЧИНСТВІ КРАЇН РОМАНО-ГЕРМАНСЬКОЇ ПРАВОВОЇ СІМ'Ї

3.1. Місце електронних документів у системі судових доказів у цивільному судочинстві Французької Республіки

Відомо, що Цивільний кодекс Франції [100] є надзвичайно давнім нормативно-правовим актом і за свою багатовікову історію мав величезну кількість редакцій. У цьому і є особливість французького законодавства, в якому норми щодо доказів містяться в основному не в Цивільному процесуальному кодексі [101], а в Цивільному кодексі.

Чинна редакція Цивільного кодексу Франції виділяє різні засоби доказування, серед яких головними є:

- Письмові докази – статті 1363 – 1380;
- Показання свідків – стаття 1381;
- Презумпції – стаття 1382;
- Визнання стороною – стаття 1383 - 1383-2;
- Присяги – статті 1384 – 1386-1.

Розвиток електронних доказів у Франції також тісно пов'язаний із електронним підписом та електронними листами, оскільки швидка поява нових комунікаційних засобів та інтенсивне використання інтернету викликали необхідність адаптації законодавства Франції до сучасних потреб.

Протягом тривалого часу письмові докази (які альтернативно називаються *preuve par écrit* або *preuve littérale*) були синонімом паперових доказів. Це було так загальновизнано, що практичної потреби в правовому визначенні не було. Проте суди зіткнулися зі зростаючими труднощами, починаючи з подання заяви до нових способів створення та збереження документів.

І лише у 2000 р. законодавець вирішив розв'язати цю проблему. Тому було вирішено, що необхідно розробити визначення письмових доказів, яке включатиме традиційні, а також електронні письмові документи.

Можна назвати три знакові дати в контексті законодавчого регулювання процесу судового доказування у Франції:

- 13 грудня 1999 р. - публікація Європейської директиви «Про систему електронних підписів, що застосовується в межах Співтовариства» [57];
- 13 березня 2000 р. - прийняття закону «Про адаптацію права доказів до інформаційних технологій, що стосуються електронного підпису»[56];
- 30 березня 2001 р. - прийняття указу «прийнятого для застосування ст. 1316-4 ЦК щодо електронного підпису» [11]

Статтею 1316 в редакції 2001 року ЦК Франції було зазначено, що «документальні докази - це докази, що складаються з серії букв, символів, цифр або будь-яких інших знаків зі зрозумілим значенням, незалежно від їх середовища та способів передачі». Викладений таким чином текст охоплює всі форми доказу, включаючи електронну [20].

Хоча це визначення модернізоване шляхом включення електронних документів, проте воно, до певної міри, залишається класичним. Зрештою, електронний лист – не більше ніж запис, записаний на альтернативному носії (відео та аудіозаписи залишаються виключені з цієї категорії). Власне, це стало звичним розрізняти «*écrits sur support papier*» та «*écrits sur support électronique*», тобто паперові документи та документи на електронній основі.

Іншими словами, будь-які докази тепер прийнятні незалежно від їх носія. Це так званий принцип нейтральності та недискримінації. Суддя не може заздалегідь відхилити електронний лист, вебскріншот, IP-адресу на тій підставі, що доказом є саме електронна пошта, вебскріншот або IP-адреса.

З іншого боку, суддя зможе відхилити його за двох умов: спочатку тому, що документ його не переконує, а потім, мотивуючи цим же, відмову. Таким чином, стаття 1316-1 ЦК Франції встановлює загальне застереження: «Написання в електронній формі визнається доказом так само,

як і запис на папері, за умови, що (...) можна належним чином ідентифікувати особу, від кого вона виходить, а також що вона складена та зберігається в умовах, які гарантують її цілісність».

Наслідок цього положення для учасника судового процесу є подвійним. Передусім, він повинен привести докази у знайому судді форму, наприклад, паперову роздруківку електронного листа. Також він повинен підготувати, упорядкувати та зберегти докази того, що наданий доказ підтверджує автентичність особи, від якої він виходить, та його цілісність. Тому потрібно організувати резервну копію поштового сервера для електронної пошти або сервера типу брандмауера, на якому будуть зберігатися листи, при чому всім керує судовий виконавець або комп'ютерний експерт, можливо, затверджений апеляційним судом.

IP-адреса лежить в основі труднощів з організацією резервної копії, оскільки вона є доказом, який надійно підтверджує особу зловмисника або комп'ютера, який намагається зламати. Оскільки IP-адреса - це дефіцитний інтернет-ресурс, стандартизований і контрольований інтернет-корпорацією для присвоєних імен і номерів ICANN. Проте статус IP-адреси такий самий, як і для будь-якого електронного доказу: він дійсно є прийнятним доказом у французькому суді. Однак повідомлення про існування IP-адреси, залишеної як слід на якомусь сервері, вимагатиме створення резервної копії журналу підключень (журналів), який зазвичай фіксує цю інформацію, створення звіту в знайомій формі, призначеної для судді, додаткове пояснення, надане самою стороною або, краще, експертом, щоб підтвердити, що сторона в судовому процесі використовує інформацію в суді справедливо [139].

Наступним кроком у запровадженні електронних доказів став Закон про правосуддя від 26 грудня 2007 року, що мав на меті модернізацію методів розгляду справи, а також Закон №1.383 про цифрову економіку від 2 серпня 2011 року, що закріпив електронні докази та визначив електронну пошту як «будь-яке повідомлення у формі тексту, голосу, звуку чи

зображення, надіслане мережею зв'язку, що зберігається на мережевий сервер або в кінцевому обладнанні одержувача» [76].

Це законодавче положення визначило умови для отримання електронної пошти й, таким чином, запропонувало значний набір доказів, доступних для сторін. Натепер електронна пошта широко використовується для направлення претензій у контексті судового процесу. Хоча цей спосіб спілкування знайшов своє місце в системі доказового права Франції, все одно існували прогалини, які слід було усунути.

Для деяких правових актів, які передбачають дійсний вияв волі сторін, закон встановлює процедуру доказування. З огляду на специфіку електронної пошти, закон передбачає обмежувальні умови для визнання її прийнятності як засобу доказування «на тих самих підставах і з такою ж доказовою силою», як написано на папері. Формалізм, встановлений законом, такий, що електронна пошта між особами рідко може бути прийнята сама по собі для підтвердження певної дії. Згідно зі ст. 1194 ЦК Франції цей формалізм може бути зменшений: якщо немає спірного питання в письмовій формі, то сторони уповноважені не доводити іншим способом. Таким чином, лист, який не відповідає суворим вимогам законодавства, може вважатися письмовим доказом.

Згідно зі ст. 1163 ЦК Франції електронна пошта може бути буквальним доказом, який «виникає з розбірливої послідовності букв, символів, цифр або будь-яких інших знаків чи символів, наділених зрозумілим значенням незалежно від їх природи, засобом або способом передачі» [100]. Для того, щоб бути визнаним доказом, він повинен відповідати умовам ст. 1163-1 ЦК Франції, тобто особа, від якої він походить, має бути належним чином ідентифікована та сам доказ має зберігатися в умовах, які гарантують його цілісність. Коли через електронну пошту вчинено юридичний акт, він повинен бути підтверджений електронним підписом, необхідним відповідно до умов статті 1163-3 ЦК Франції. Положення статті 279 Цивільного процесуального кодексу Франції, що застосовуються до перевірки написання

актів за особистим підписом, повторюють формальні вимоги ст.ст. 1163-1 і 1163-3 ЦК Франції.

Електронний підпис, безперечно, є невід'ємною частиною електронного листа. Це не є результатом номінальної адреси електронної пошти чи простого зазначення імені автора в кінці електронного листа чи навіть проставлення відсканованого підпису. Згідно зі ст. 1163-3 ЦК Франції він полягає «у використанні надійного процесу ідентифікації, що гарантує його зв'язок із діями, до якого він приєднаний». Такий процес вважається надійним, якщо він гарантує ідентичність підписанта та цілісність документа.

Коли нормативні вимоги зафіксовані й дотримані, використання цього передбачуваного надійного електронного підпису дозволяє електронній пошті набути повної доказової сили і, зокрема, сприяє укладенню договору електронними засобами. Оскільки ця презумпція має спростовуватися, то той, хто заперечує електронний лист із таким підписом, повинен надати докази того, що використаний процес підпису не був надійним.

Ця презумпція на практиці часто виявляється «технологічно» неспростовною з огляду на труднощі надання доказів протилежною стороною і потребує значних фінансових ресурсів. Цей механізм на практиці може виявитися навіть небезпечним, особливо якщо позитивне право ігноруватиме поняття електронного шахрайства, що позбавляє учасника судового процесу належних засобів захисту. Усвідомлюючи потенційну небезпеку, законодавець не визнає чинності окремих видів правових актів, укладених за допомогою електронних засобів. Згідно зі ст. 963-2 ЦК Франції не можуть бути вчинені електронними засобами правочини, що стосуються сімейного та спадкового права, особистої чи речової безпеки, цивільного чи господарського характеру, крім тих, що вчинені у професійній сфері [151].

За відсутності електронного підпису лист, направлений на електронну пошту, не завжди визнається письмовим доказом, а з іншої сторони - його доказова сила не завжди зменшується.

У Франції саме судова практика прояснила долю простого електронного листа без електронного підпису. У широко розповсюдженому рішенні Касаційний суд підтвердив, що за відсутності надійного процесу ідентифікації підпису простий електронний лист, автентичність якого оспорується, не може вважатися доказом [94]. Суддя не може зробити висновок з адреси електронної пошти про ідентифікацію автора повідомлення [158]. Це широко прокоментоване рішення не є одностайним [173] і підкреслює бажання Касаційного суду ухвалити одностайне рішення шляхом суворого застосування положень, що стосуються дослівних доказів. За відсутності електронного підпису електронна пошта просто не буде вважатися «ідеальним» письмовим доказом [126].

Таким чином, електронна пошта не позбавлена доказової сили і, за умови достовірності стверджуваного факту, як це передбачено ст. 1194 ЦК Франції, вона може бути початком письмового доказування. Потім його потрібно буде доповнити іншими доказами, такими, наприклад, як показання свідків.

Враховуючи той факт, що електронна пошта стала звичайним способом спілкування, аж до того, що вона замінила більшість традиційних листів, формалістичні рамки, встановлені законом, можуть спонукати сторони відступати систематично за «чисто формальним питанням» заперечувати попереднє зобов'язання і розпалювати недобросовісність. Щоб обійти цю пастку, можна було б розглянути запит на збереження доказів за допомогою судового виконавця, подавши запит до голови Трибуналу [157]. Доказова цінність електронної пошти була б відновлена за допомогою судового виконавця та за допомогою комп'ютерного експерта, який зазначав би наявність електронних листів на сервері особи, яка заперечує їх існування або автентичність.

Юридична консекція електронного листа на ст. 1163 ЦК Франції знімає сумнів щодо прийнятності електронного листа як доказу. Це уточнення є

особливо своєчасним у темі, де його використання є дуже частим. Суворе дотримання умов ст.ст. 1163-1 і 1163-3 ЦК Франції не є необхідним, оскільки в комерційних справах безсумнівне доведення спеціально не вимагається на підтвердження вимог, а достатньо звичайної переваги доказів. Рішення апеляційного суду нагадує про цей принцип свободи доказів у комерційних справах і підтверджує, що письмове повідомлення, яке не відповідає всім вимогам законодавства, не позбавлене доказової сили, оскільки воно було підписане комерційною компанією, до якої застосовувалися лише положення ст. 74 Торгового кодексу Франції. Французький касаційний суд, відповідно до цього принципу свободи доказів у комерційних справах визнав незабезпечений електронний лист як доказ [95; 197]. Також у рішенні уточнюється, «що не дозволяється оскаржувати метод доказування лише на тій підставі, що він заснований на електронному письмі». Прецедентне право комерційної палати Французького касаційного суду багате на інформацію і дозволяє нам прояснити, як розуміти електронну пошту в питаннях, де докази є безсилі.

У багатьох інших випадках, коли трейдери ведуть бізнес з не трейдерами, суворий формалізм може бути проблематичним. На сьогоднішній день багато осіб не мають інструментів для видачі електронних підписів, тоді як використання електронної пошти є дуже поширеним в їхніх відносинах із трейдерами. Наприклад, зазвичай клієнти терміново звертаються до свого страхового агента після придбання транспортного засобу та замовляють одразу гарантію електронною поштою, що ставить продавця в делікатну ситуацію: бажаючи задовольнити свого клієнта в поспіху, йому часто доводиться нехтувати захистом від листів в розумінні закону. Нерідкі випадки, коли клієнт потім намагається уникнути цього зобов'язання, знайшовши більш вигідний контракт з іншою компанією. Електронна пошта не зможе бути протиставлена йому, навіть якщо протягом цього періоду часу на його автомобіль буде надано

гарантію. Закон у цьому сенсі не дав можливості сприяти такому типу відносин, що вимагало б більшої гнучкості та швидкості [122].

З іншого боку, кодекс був доповнений новою ст. 1163-2 ЦК Франції відповідно до конвенції про доказування [164]. Після цього можна було б уявити, що в рамках своїх відносин трейдери та неторгівці заздалегідь передбачають, що електронні листи визнаються доказами між ними. Тоді укладення такої угоди дає можливість обійти суворий формалізм закону.

Для правових актів, що стосуються правочинів на суму менше 1140 євро, ст. 1188 ЦК Франції не потребує письмового документа. Таким чином, простого електронного листа, який не має електронного підпису в розумінні закону, буде достатньо, щоб підтвердити трансакцію невеликої суми. Згідно зі статтею 279 ЦПК, якщо такий електронний лист оскаржується, суддя має перевірити, чи встановлено його відповідно до положень статей 1163-1 та 1163-3 ЦК. Парадоксально, але суддя потім перевірить електронну пошту, яка вважається приватною, навіть якщо вона не була підкріплена електронним підписом. З цією метою він може наказати сторонам передати всі наявні в них комп'ютерні сліди, які були б корисними для вирішення спору, і він може доручити експерту шукати зазначені сліди в будь-якій комп'ютерній системі, де вони можуть бути знайдені.

Слід зазначити, що важко уявити, що на таку малу суму, як для Франції, виділяється стільки ресурсів. Однак, якщо електронний лист не відповідає усім цим умовам, його не включають в обговорення. Суддя може прийняти це як початок доказування в письмовій формі. Оскільки «досконалий» доказ у справі не вимагається, цього доказу може бути достатньо, щоб переконати суддю [126].

Багато електронних листів використовуються для підтвердження вини. У рішенні від 16 березня 2000 р. [224] суд із трудових спорів постановив, що електронний лист, надісланий працівником із поштової скриньки його роботодавця, демонстрував загрозливу поведінку, яка «може серйозно поставити під загрозу довіру» до компанії, яку він представляв та

безсумнівно, становила серйозну провину. У рішенні від 9 червня 2005 р. [222] суд першої інстанції, вирішуючи як суд апеляційної інстанції трудового суду, постановив, що різні електронні листи, надіслані працівником усім співробітникам, були повідомленнями «обурливого характеру» і продемонстрував "провокаційне ставлення сумнівних дій». Працівника все ж було звільнено з поважної причини. Ці електронні листи були отримані як дійсний доказ для характеристики вини, але в даному випадку вони не були оскаржені. Навіть у разі спору видається, що відсутність електронного підпису не впливає на їх доказову силу, оскільки дія статті 1163-3 ЦК стосується не лише правових актів, які є юридичними документами, а і правових наслідків. Оскільки вина є юридичним фактом, який можна довести будь-яким способом, суддя владно оцінюватиме прийнятність електронного листа, не обов'язково застосовуючи положення статей 1163 та наступних Цивільного кодексу [122].

Потреба в цій гарантії змусила законодавця встановити дуже формальні умови щодо його прийнятності. Рекомендується, навіть у питаннях юридичних фактів, підходити до цих доказів з особливою обережністю. У рішенні, винесеному 11 квітня 2013 року [223], суд першої інстанції прийняв прості скріншоти як доказ, щоб звинуватити подружжя у вчиненні правопорушення. У цьому випадку посилання між користувачем і сайтом знайомств здійснюється за допомогою псевдоніма та пароля, зазначених на Post-it. Критерії ідентифікації, використані тут, здаються легкими та недостатніми з огляду на останні законодавчі положення, спрямовані саме на забезпечення використання електронного листа. Конкретні формулювання статей, що стосуються електронного листа, яскраво демонстрували бажання якнайкраще гарантувати ідентифікацію їх автора. Якщо ці положення стосуються лише підтвердження договірних зобов'язань і зобов'язань про оплату, тим не менш, здається, що *ratio legis* закликає нас виявляти стільки запобіжних заходів і в інших питаннях.

Як можна спостерігати, у Франції особлива цінність письмової форми для підтвердження правового акту змусила законодавця під впливом європейського законодавства швидко визнати доказову цінність письмового тексту та електронного підпису [112].

Відповідно до виразу «функціональної еквівалентності», електронний лист можна було б уподібнити паперовому письму в тому сенсі, що він виконував ті ж самі функції доказу, як сам лист [135]. Згодом розвиток цифрових технологій призвів до появи нових методів випробування: геолокації, захоплення комп'ютерних даних, створення баз даних, що дозволяють зберігати докази та здійснювати перехресний пошук між файлами даних поліції та органів правосуддя.

Поступово за допомогою цифрових технологій було отримано багато традиційних способів доведення, які виникли в результаті аналогічних процесів. Так відбувається із записом зображень, розмов та спілкування, який зараз оцифрований. Так само в компаніях документація більше не зберігається лише в паперовому форматі. Тепер все інтегровано в «інформаційну систему», яка повністю складається з цифрових даних, незалежно від форми вираження: лист, звук, зображення тощо. У всіх сферах, які стосуються цих компаній, сьогодні основний акцент полягає в доступі до інформаційної системи, щоб зібрати докази, корисні для вирішення спору.

Ця зміна суттєво впливає на характер доказів. Докази більше не обов'язково впливають із речей у матеріальному сенсі цього терміну. Доказ перетворився на «число», природа якого є неістотною і набуває форми послідовності 0 і 1. Ось очевидна унікальність і простота електронного доказу.

Згідно з рекомендаціями Ради Європи, «електронні докази» означають будь-які докази, які виникають на основі даних, що містяться або створюються пристроєм, робота якого залежить від програмного забезпечення або даних, що зберігаються чи передаються в системі чи пристрої, комп'ютерної мережі» [27].

Спільним між всіма визначеннями електронних доказів є дані. У більшості ці дані мають бути пов'язані з програмним забезпеченням або комп'ютерною мережею, іншими словами, з комп'ютерною системою. У Регламенті Європейської комісії дані мають властивість зберігатися в електронній формі. Таким чином визначення стосуються одних і тих самих даних: цифрових даних. Це значення є проблематичним. З технічної точки зору всі електронні докази мають однакову форму. З точки зору доказового права, електронні докази мають дуже різні форми й порушують дуже різні питання, які поняття «дані» не в змозі відобразити.

Справді, між даними геолокації мало спільного, що може спричинити проблеми порушення конфіденційності та даних електронного підпису, що викликає питання щодо ідентифікації особи, яка підписує, та згоди, яку вона виражає своїм підписом. Іншими словами, притягувати особу до відповідальності на основі географічного положення, що зберігається в базі даних, і намагатися ідентифікувати зміст контракту, закріпленого в blockchain, підпадає під два дуже віддалених процеси доказування, як щодо питання доказів, так і правил, застосовних до процедури, яка, ймовірно, буде реалізована в цих двох ситуаціях [139].

Проблеми, пов'язані з появою цифрових технологій у сфері доказування, неоднакові залежно від використовуваних методів доведення. Наприклад, коли зображення редагується у відео, воно залишається зображенням, незалежно від того, чи є режим запису та зберігання цифровим чи аналоговим. Воно показує ту саму людину або ту саму сцену. В обох випадках його можна сфальсифікувати, а експертиза може допомогти перевірити його справжність. Іншими словами, техніка змінюється, але вона не змінює основ процесу доведення та труднощі, які створює метод доведення. І навпаки, поява електронного листа в цивільних справах спричинила справжню зміну парадигми. Електронний підпис, що ідентифікує його автора, не має ознак власноручного підпису. Прикріплюється простим клацанням миші або введенням секретного

коду. Воно набуває вигляду ряду цифр, незрозумілих як для автора, так і для одержувача, і не відображається в графічному вигляді. Якщо він має характеристики кваліфікованого електронного підпису, він несе презумпцію надійності [75]. Тоді тягар доведення автентичності підпису змінюється, тому доведення особи автора діяння не тільки набуває іншої форми, а й вимагає дотримання специфічного правового режиму.

Наприклад, кваліфікований електронний підпис можна протиставити його автору. Тоді останній має продемонструвати відсутність автентичності. І навпаки, власноручний підпис може бути поставлений під сумнів за допомогою простої процедури відмови в письмовій формі, яка де юре руйнує автентичність способу доказування.

Дані, яких може стосуватися судова заборона, дуже різноманітні. Це можуть бути дані, що стосуються особи абонента, типів послуг, які він використовує, його доступу до служби онлайн-зв'язку, місцезнаходження його пристрою. Це також можуть бути метадані електронних комунікацій або дані, що стосуються вмісту. Даних захід охоплює комп'ютерні пошуки, вторгнення в комп'ютерні системи (взлом), геолокацію терміналів, «фадети», історію перегляду, збережені електронні повідомлення тощо. Іншими словами, судова заборона охоплює цілий набір методів доказування з метою застосування до них єдиного правового режиму, який можна позначити виразом «захоплення комп'ютерних даних» [132].

У рекомендаціях Ради Європи саме сторони надають електронні докази в суді. Тому суддя має прийняти ці докази, беручи до уваги труднощі, які впливають з їх природи: їх автентичність, технічні проблеми, пов'язані з їх збиранням, способом оцінки їх доказової цінності. І навпаки, у запропонованому регулюванні саме суддя виступає з ініціативою шукати докази там, де вони є. Таким чином, текст регулює труднощі, пов'язані з цим дослідженням: з одного боку, відносини між суддею та постачальником послуг, з іншого боку, необхідність збереження прав осіб, яких цікавлять ці дані,

Поява цифрових технологій і те, як ця технологія вторглася в юридичний світ, схоже, охопили всі електронні докази і, як вбачається, містить усі дані, які можуть знадобитися судді для визначення фактів. Цифрові технології суттєво змінили науку та закони щодо доказів, проте це не допустило появи нової концепції, яку ми б назвали електронним доказом. З іншого боку, це додало б складності правовзастосовчій практиці [139].

Цей розвиток не є завершеним, оскільки цифрові докази, у своїй різноманітності, ще можуть багато чого додати до процесу встановлення юридичних фактів без необхідності використання назви «електронних доказів» для їх ідентифікації та регулювання.

Наприклад, слід відмітити, що 20 листопада 2020 року міністр юстиції Франції підписав наказ (JUST2030158A) щодо електронного підпису судових рішень, ухвалених у цивільних справах. Це рішення забезпечує технічну основу для електронного підпису судових рішень і може передбачати те, що необхідно для розвитку цифрових доказів в подальшому.

Указ від 20 листопада 2020 року втручається, зокрема, в рамки регламенту (ЄС) 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та рішення про виконання (UE) 2015/1506 Комітету від 8 вересня 2015 року про встановлення специфікацій щодо форматів удосконалених електронних підписів і вдосконалених електронних печаток, які визнаються органами державного сектору, зазначеними в пункті 5 статті 27 та в статті 37, § 5, вищезгаданого регламенту 910/2014.

Рішення торкнулось статей 1366 та 1367 ЦК Франції, які на даний момент передбачають, що електронний лист має таке ж доказове значення, як лист на папері та встановлює рамки для ідентифікації автора електронного підпису.

У тексті, зокрема, передбачено, що будь-який процес, який використовується для накладання електронного підпису до судових рішень,

зазначених у статті 456 Цивільного процесуального кодексу, реалізує кваліфікований електронний підпис у значенні вищезгаданого європейського регламенту 910/2014.

Цей указ є важливим кроком у цифровізації цивільного судочинства. Справді, цей процес електронного підпису дозволяє публікувати цивільні рішення (суди, промислові трибунали та апеляційні суди, за винятком господарських судів, які мають певну автономію) без необхідності їх друкувати, підписувати вручну та потім сканувати для сповіщення та архівування.

Воно повторює постанову від 18 жовтня 2013 року щодо електронного підпису судових рішень, ухвалених у цивільних справах Касаційним судом (перше рішення, підписане електронним підписом від 13 жовтня 2013 року) та ухвалу від 9 квітня 2019 року щодо електронного підпису рішень господарських судів [64].

Таким чином, цей процес неодмінно заощадить час, а також забезпечить читабельність щодо впровадження відкритих даних. Це також має спрощувати формальності повідомлення для юристів, які керуються поштою та архівами.

Він заснований на системі аутентифікації електронного підпису, стандартизований на європейському рівні, що також дає змогу сприяти безпеці та надійності рішень та їх взаємному визнанню, зокрема в межах Європейського Союзу.

Ця реформа в майбутньому повинна дати можливість полегшити завдання процедур обробки, покращення якості процедур, збереження якості доказів, зокрема зібраних зображень, а отже, їх ефективності та швидкості. Крім того, це може сприяти розгляду складних ситуацій, які вимагають, наприклад, перехресної перевірки інформації [228].

Таким чином, прогрес, досягнутий у судових рішеннях, має слугувати прискорювачем для модернізації цифрового цивільного судочинства, яке

вимагає якнайшвидшого завершення, щоб якнайшвидше забезпечити його ефективне впровадження.

На шляху до прискорення оцифровки систем та їхньої взаємодії в рамках європейського судового співробітництва необхідне прискорення електронної модернізації цивільного та кримінального судочинства.

На цій основі 30 липня 2020 року Європейська Комісія прийняла дорожню карту, яка висвітлює проблему, по суті, паперового судочинства та використання методів передачі, які впливають на доступ до правосуддя, на шкоду громадянам і бізнесу, тим більше в середовищі, деградованому через кризу охорони здоров'я. У цій дорожній карті підкреслюється, що оцифрування правосуддя є важливою умовою для покращення якості судових систем у цивільних і кримінальних справах, зокрема в контексті транснаціональної злочинності, як зауважив Європол [19].

Тому Європейська Комісія розпочала консультації, які мають призвести до прийняття повідомлення про оцифрування правосуддя, яке має бути представлено найближчим часом і заявленою метою якого є, зокрема, прискорити оцифрування систем та їх сумісність у рамках судової співпраці, яка становить юридичну основу для діяльності Європейського Союзу [228].

3.2. Сутність та доказова сила електронних доказів за законодавством та правовою доктриною Федеративної Республіки Німеччина

Німецьке цивільне процесуальне законодавство не знає правових перешкод для доказування за допомогою електронних доказів. Електронні докази є допустимими доказами і вони підлягають візуальному або експертному засвідченню. Візуальні докази можуть розглядатися судом, оскільки сам суд бере до уваги візуалізований вміст електронного файлу. Експертне засвідчення використовується, якщо візуалізації не достатньо для переконання в автентичності файлу.

Що стосується доказового права для електронних документів, то законодавство Федеративної Республіки Німеччина (далі – ФРН) містить одне з найбільш ліберальних з усіх можливих правил. Навіть якщо, з точки зору матеріального права, ефективність використання доказу залежить від дотримання письмової форми, дотримання письмової форми може бути доведено всіма іншими можливими доказами. Допустимість засобів вирішується в контексті принципу вільної оцінки доказів, а не під час їх визнання як доказів.

Правові норми доказів у німецькому законодавстві є анахронічним залишком, а реконструкція правил доказів для документів показала, що зазвичай вирішальні питання щодо автентичності, справжності та достовірності документа підлягають вільній оцінці доказів і на них не поширюється жодне правило доказування [79].

Основою цивільного процесуального права у ФРН є Цивільний процесуальний кодекс ФРН, згідно з яким не потребує доведення: все, що безперечно; все, що визнано, – § 307 ЦПК ФРН; загальновідомі факти – § 291 ЦПК; презумпції, встановлені законом, - § 292 ЦПК ФРН; прямо не оскаржені факти й цим визнані факти — абз.3 § 138 ЦПК ФРН [81]. У німецькому цивільному процесі метою збирання доказів виступає формування суддівського переконання в істинності спірного твердження [234]. У процесі збирання доказів, за винятком випадків, коли суд за ініціативою має право збирати докази (§ 448 ЦПК ФРН), пріоритет повністю віддається розсуду сторін.

Під тягарем доказування в цивільному процесі Німеччини розуміється ризик програшу процесу, що лежить на стороні, у разі недоведеності фактичних тверджень даної сторони [234]. У літературі вказується на те величезне значення і «небезпечний» характер тягара доказування, який називається часто «Rückgrat des Prozesses» («хребет процесу»). При цьому зазначається, що тягар доказування може бути як суб'єктивним, так і об'єктивним. Суб'єктивний тягар доказування означає необхідність

запобігання програшу процесу довести все, що є спірним і важливим для переконаності суду в істинності фактичних тверджень. У свою чергу, об'єктивний тягар доказування розуміється як загальний ризик програшу процесу через недоведеність [199].

У ЦПК ФРН існує «неписане» основне правило розподілу тягара доказування, розроблене судовою практикою і сформульоване наукою цивільного процесу, згідно з яким особа, яка звернулася з вимогою, несе тягар доказування правовстановлюючих фактичних тверджень, а протилежна сторона, на відміну від цього, тягар доказування правоприпиняючих, що виключають або перешкоджають здійсненню права фактичних тверджень [199; 90]. Інакше кажучи, кожна сторона доводить сприятливі їй фактичні твердження.

Особливий інтерес, з урахуванням теми дисертаційного дослідження, становить розподіл тягара доказування з електронними доказами.

Питання, на яке слід звернути увагу і відокремити від прийнятності електронних документів, це тягар доказування і зобов'язання сторін судового процесу та третіх сторін поза процесом співпрацювати при наданні доказів за допомогою електронних документів. Це питання може виникати в найрізноманітніших контекстах. Цілком можливо, що сторона, на яку покладено тягар доведення, захоче надати докази за допомогою власних електронних документів або електронних документів третіх осіб. Іноземні документи можуть перебувати в розпорядженні протилежної сторони, сторони, на яку не покладено тягар доведення, або бути в розпорядженні третьої особи.

Якщо сторона, на яку покладено тягар доведення, бажає надати докази за допомогою власних електронних документів, вона повинна не лише надати суду (й опоненту) доступ до відповідного документа (зазвичай починаючи з здійснення комп'ютерної роздруковки), але також необхідно розкрити всю інформацію, необхідну для перевірки надійності, і в цьому контексті надати суду або судовому експерту доступ до самої системи. Якщо

вона цього не зробить, вона ризикує не мати можливості надати належні їй докази та програти процес через те, що тягар доведення покладається на неї. У цьому відношенні тягар доведення регулює рівень активності та участі, бажаний для встановлення істини.

Якщо сторона, на яку покладено тягар доведення, хоче надати докази за допомогою електронних документів, якими володіє опонент, модель тягаря не працює. Відповідно до принципу процесуального права "*Nemo contra se edere tenetur!*", так би мовити, згідно з природним правом, ніхто не повинен пред'являти документи проти самого себе. Таким чином, опонент у судовому процесі міг, незважаючи на несприятливу ситуацію з доказами, залишити іншу сторону без доказів і через відсутність співпраці перемогти в судовому процесі. Цей результат приймається деякими судами, принаймні в більш м'якій формі. Принцип інколи може бути обмежений з огляду на суттєву правову інформацію і допускаються мінімальні виправлення в рамках моделі тягаря, а також на самій моделі шляхом зменшення тягаря обґрунтування сторони, на яку покладено докази, з одночасним збільшенням тягаря обґрунтованого захисту сторони, не обтяженої доказами [5; 168].

Інші ж намагаються вказати шлях до «процесуальної сучасності» німецького цивільного судочинства та виправдати загальний процесуальний обов'язок для сторони, яка не несе тягаря доведення, надавати інформацію та співпрацювати.

Знову ж таки, тут існує суперечка щодо віднесення електронних доказів до сфери речових доказів або існують в області документальних доказів. Якщо дотримуватися більш суворих зобов'язань щодо розкриття інформації та співпраці, то повинні застосовуватися документальні докази, якщо менш суворі, то речові докази. Таку позицію розвинули німецькі юристи, які з поважних причин приймають сторону щодо загального обов'язок публікувати документи. Однак, як у випадку з доказовою силою електронних доказів, суперечка щодо присвоєння тягаря доказування здається малоплідною. З одного боку, незважаючи на розвиток цієї суперечки

в цивільній процесуальній догматиці, немає абсолютно ніякої згоди щодо загального обов'язку публікувати документи, що виходить за рамки правил §§ 422 і 423 ЦПК ФРН. Навпаки, багато виступають за обмеження можливостей, викладених у розділах 143, 273 (2) ЦПК ФРН.

Важливо попроситися з принципом: «*Nemo contra se edere tenetur!*» у німецькому процесуальному праві. Справедливі рішення мають прийматися лише на основі правдивості фактів, на яких базується рішення. І кожна зі сторін спору зобов'язана виконати свою частину, щоб переконатися, що рішення є єдиним істиним. Доведеться погоджуватися на привілеї та часто входити в процес зважування конкуруючих принципів справедливості. Однак тягар обґрунтування доказів не може покладатися в односторонньому порядку на процедурне роз'яснення та повинно існувати зобов'язання щодо співпраці сторони, яка не має тягаря доведення.

Кожен, хто, як і традиційне німецьке процесуальне право та прецедентне право німецьких судів, продовжує сповідувати принципу: «*Nemo contra se edere tenetur!*», залишається залежним від використання виняткового потенціалу електронних доказів у розпорядженні протилежної сторони. Ця сторона повинна шукати матеріально-правові претензії, знаходити спеціальні процесуальні норми, враховувати обсяг тягаря обґрунтування для тверджень і контртверджень і, можливо, вдаватися до інструменту фрустрації доказів із його процесуальними санкціями.

Нарешті, залишається без відповіді питання про те, як сторона, яка несе тягар доведення, може представити докази, використовуючи електронні докази, які знаходяться у володінні третьої сторони, яка не бере участі в провадженні. Німецьке процесуальне законодавство також не дає відповіді на це. У разі документальних доказів, а також речових доказів, треті сторони, які не беруть участь у процесі, можуть бути притягнуті до відповідальності, лише якщо пред'явник має право на пред'явлення документів або на дозвіл перевірки третьої сторони.

З юридичної точки зору ця норма провальна, оскільки закриває можливість для роз'яснення та стоїть у невіршеному протиріччі з майже необмеженим обов'язком кожної третьої сторони. Зрештою, немає жодного виправдання, чому не потрібно показувати те, про що можна змусити говорити примусово. Комісія з цивільно-процесуального права правильно подала пропозицію щодо поправки, яка, відповідно до обов'язку давати свідчення, також зобов'язувала третіх осіб пред'являти або зберігати документ наготові [18]. На жаль, § 378 ЦПК ФРН, який був включений до Цивільного процесуального кодексу, не враховує це, на свідка покладено лише обов'язок «переглянути записи та інші документи та взяти їх із собою на зустріч, якщо це дозволено та розумно». У цьому відношенні посилання на основні обов'язки свідка щодо розкриття інформації, викладені в розділі 429 ЦПК ФРН. Параграф 378 (1) ЦПК ФРН не містить жодного розкриття інформації, а лише зобов'язання освіжити та підтримувати спогади, що, звичайно, також стосується комп'ютерних роздруківок та електронних доказів.

У літературі докази прийнято поділяти за такими критеріями:

- за метою - на повні докази та докази переважної ймовірності твердження;
- за порядком дослідження - на суворі та вільні докази;
- за метою самих доказів - на основні докази та докази, подані до суду для спростування інших доказів;
- за характером доказів - на прямі та непрямі докази [199].

Повним доказом вважається такий доказ, коли суд повністю переконаний в істинності фактичного твердження. На відміну від цього, про доказ переважної ймовірності твердження може йтися в разі існування лише певної міри переконаності в істинності фактичних тверджень. Відповідно до §284 ЦПК ФРН суд при дослідженні доказів повинен суворо дотримуватися приписів §355-484 ЦПК ФРН. Такий порядок дослідження доказів у німецькому процесуальному праві вважається суворим доказом. Якщо ж

йдеться про вільний доказ, то суд не пов'язаний як передбаченими ЦПК ФРН засобами доказування, так і існуючими правилами дослідження доказів. Слід зазначити, що цей вид доказів законодавчо не передбачений, а був, згідно з панівною точкою зору в процесуальній літературі, розроблений для встановлення процесуальних передумов та передумов для оскарження, у тих стадіях процесу, де не проводяться усні судові засідання. До них відносяться: ухвала про дослідження доказів до усного розгляду щодо надання офіційних довідок - §358a ЦПК ФРН, судові звернення до органів влади або до посадових осіб із запитом про надання документів або офіційних довідок - №2 абз.2 §273, порядок дослідження іноземного права - §293, а також провадження за клопотанням про надання допомоги для сплати процесуальних витрат - §118.

З метою прискорення та спрощення судочинства та впровадження нових інформаційних технологій у процес, першим Законом про використання електронних форм комунікації в судочинстві (Justizmodernisierungsgesetz) була передбачена можливість дослідження судом доказів так, як йому видається зручним (тобто йдеться про вільний доказ) за наявності згоди сторін [152]. Отримання такої згоди означає для суду можливість відхилитися від обов'язкових розпоряджень ЦПК ФРН. При цьому така згода не повинна обов'язково стосуватися всього процесу дослідження доказів, а може обмежуватись окремими діями з дослідження доказів. З точки зору законодавця, ця норма уможливить, наприклад, проведення додаткового допиту свідка за телефоном або електронною поштою [89].

Основними доказами прийнято вважати ті докази, які повинні свідчити про наявність елементу юридичного складу норми права, що застосовується, а також про істинність тверджень сторони, на якій лежить тягар доказування. У свою чергу, доказами, поданими до суду для спростування інших доказів, є докази, які протилежна сторона наводить для підтвердження неістинності або як заперечення щодо фактичного

твердження. Основні докази можуть наводитися з використанням будь-яких засобів доказу; для доказів, поданих до суду для спростування інших доказів, згідно з абз.2 §445 ЦПК ФРН, встановлено заборону на допит сторони.

Нарешті, останнім підрозділом видів доказів виступає поділ доказів на прямі та непрямі. Прямий доказ містить факти, які мають безпосередньо свідчити про наявність чи відсутність окремого елементу юридичного складу [199]. У свою чергу, непрямі докази мають у своєму змісті інші факти, що не мають прямого відношення до юридичного складу й виникають у процесі тільки після констатації наявності або відсутності окремого елементу юридичного складу. До таких доказів належать, так звані, допоміжні факти, що стосуються допустимості чи доказової сили засобу доказування.

Під засобами доказування в цивільному процесі Німеччини розуміються носії безпосереднього зорового сприйняття чи передачі: речові докази, документи, свідок, експерт, сторона. Слід зазначити, що цей перелік із п'яти видів засобів доказування скор. «ZUSAP» не є вичерпним. Судовою практикою були вироблені інші засоби доказування, що не належать до жодного з перерахованих вище. До них відносяться офіційні довідки органів влади та посадових осіб, а також рівнозначні їм офіційні заяви посадових осіб, які мають відмовляючий, що перешкоджає або забороняє характер, навіть у тих випадках, коли вони були видані/вчинені не за розпорядженням суду. До інших засобів доказування відноситься також свідоцтво органу влади, який виконував доручення, яке згідно з абз.2 § 183 ЦПК ФРН необхідно для доказу доставки за кордон засобами, передбаченими пп. 2 та 3 абз.1 даного параграфу. Перелічені докази не є письмовими доказами, а оцінюються судом у межах вільних доказів.

Як один з основних принципів цивільного процесу прийнято виділяти, закріплений § 286 ЦПК ФРН принцип вільної оцінки доказів [234]. Відповідно до абз.1 названого параграфу суд, беручи до уваги зміст розгляду в цілому та результат дослідження доказів, вирішує на своє переконання, чи слід вважати фактичне твердження істинним чи ні. Крім того, згідно з абз.2

§286 суд пов'язаний лише законодавчо встановленими правилами оцінки доказів, передбаченими ЦПК ФРН. До таких випадків належать §415-418 ЦПК ФРН про приватні та офіційні документи. Йдеться про, так звані, встановлені докази, вільна судова оцінка доказового значення яких обмежена. Так, приватні документи, підписані укладачем або нотаріально засвідчені відповідно до §416 ЦПК ФРН є повним доказом того, що заяви, що містяться в них, виходять від укладача. У свою чергу офіційні письмові документи мають найвищу доказову силу, будучи згідно §417 ЦПК ФРН, повним доказом свого змісту. Дані правила про доказову силу письмових доказів є винятком із принципу вільної оцінки доказів.

Даний принцип цивільного процесу прийшов на зміну існуючому раніше формальному процесу доведення в загальному та канонічному праві [119]. У зазначеному процесі діяв принцип: «тільки два свідки кажуть правду». Будь-яке відхилення від встановленої форми вело до програшу процесу, заїкуватість або дефект промови могли призвести до недійсності показань під присягою, за відсутності двох свідків необхідним елементом у процесі виступало визнання сторони, задля чого часто необхідно було вдаватися до катування [205].

Вперше принцип вільної оцінки доказів згадується в часи Просвітництва, а до теперішнього часу він вже знову обмежується такими «чинними правилами доказування», як очевидні (безперечні) докази, тягар доказування, випадки перерозподілу тягара доказування. Важливим елементом свободи є переконання суду в істинності фактичного твердження. Для доказу певного ходу подій у процесуальній літературі вказується на те, що однієї суб'єктивної переконаності судді недостатньо, але також не потрібно й абсолютної достовірності [71].

Потрібна від суду переконаність, згідно з § 286 ЦПК ФРН, має три ступені. Проста ймовірність потрібна відповідно до абз. 1 § 294 для підтвердження фактичного затвердження і, в порівнянні з повним доказом, пред'являє менші вимоги при формуванні переконання в судді. Фактичне

твердження вважається доведеним, коли є перевага. У процесі доведення допустимі будь-які засоби доказування, у тому числі засвідчення, що замінює присягу. Більш висока міра ймовірності (т.зв., що межує з достовірністю) існує в тому випадку, коли відсутні сумніви в розумної та розсудливої людини з приводу доведеності фактичного твердження. Такий ступінь переконаності судді є достатнім для висновку експерта. Дуже висока ймовірність як ступінь суддівської переконаності потрібна в особливих, зазначених у законі випадках і, насамперед, у процесах встановлення походження особи (напр. позов про встановлення походження дитини). Крім цієї шкали, у процесуальній літературі прийнято виділяти якісну й кількісну ймовірність. Традиційно до кількісної ймовірності прийнято відносити результати вимірювань у медичному дослідженні, які може обійти не один суддя. У свою чергу, до якісної ймовірності ставиться питання про те, чи збрехав на допиті свідок. Коли остання має лише два варіанти відповіді – «так» чи «ні», кількісна ймовірність може виражатися у відсотковому співвідношенні. І тут статистика служить підставою переконаності [124].

При доведенні у сфері електронного документообігу можливі обидва види ймовірності. Так, доведення ідентичності електронного документа пов'язано з кількісною ймовірністю і здійснюється за допомогою криптографічного методу. При вирішенні питання нефальсифікованості електронного документа матиме значення якісна ймовірність, оскільки тут виникають питання надійності (як у випадку зі свідком) та незмінності документа.

Розгляд питання про електронний підпис у доказовому праві Німеччини доцільно розпочати з подання основних положень та цілей Директиви ЄС 1999/93/ЄС, оскільки Закон ФРН від 16.05.2001 «Про електронний підпис» базується саме на цьому документі.

Основною метою прийняття Директиви ЄС 1999/93/ЄС було подолання відмінностей у правовому регулюванні електронних підписів окремих держав- членів ЄС, а також відповідно до ст. 1 Директиви, полегшення їх

використання та сприяння правовому визнанню [194]. Крім цього, прийняття Директиви ЄС 1999/93/ЄС переслідувало мету загального визнання методу електронної ідентифікації та поставило перед державами - членами ЄС завдання гарантувати використання електронного підпису як доказу у судочинстві (п.21 преамбули). Відповідно до ст. 2 Директиви ЄС «Про загальні принципи електронних підписів» передбачається три рівні (види) електронних підписів: простий, «удосконалений» та кваліфікований електронний підпис.

Згідно з п.1 ст.2 названої Директиви під простим електронним підписом розуміються дані в електронній формі, які додаються або логічно поєднані з іншими електронними даними та служать як метод розпізнавання. Таким чином, під зазначене визначення підпадають будь-які відомості в електронній формі, які допускають можливість встановлення їх автора, а саме: надруковане в кінці ім'я автора або відсканований особистий підпис. Інших вимог до безпеки в даному випадку не передбачено. Директива прямо не передбачає поняття «розпізнання». У науковій літературі під розпізнанням у сенсі Директиви ЄС 1999/93/ЄС розуміється встановлення автора повідомлення.

Правове значення простого електронного підпису, відповідно до п.2 ст.5 Директиви полягає лише в тому, що держави — члени ЄС повинні гарантувати, що електронний підпис не втратить свого правового статусу та допустимості як доказу в судочинстві лише тому, що: (а) існує в електронній формі, (b) не заснований на кваліфікованому сертифікаті, (c) не заснований на кваліфікованому сертифікаті, виданому акредитованим сертифікуючим сервіс-провайдером (центром), або (d) не створений надійним пристроєм створення електронних підписів.

«Удосконалений» електронний підпис, так само як і простий електронний підпис, є технічно відкритим, що означає відсутність необхідності асиметричного способу шифрування даних [193, с. 39]. Відповідно до п. 2 ст. 2 Директиви «просунутий» електронний підпис

повинен задовольняти наступні вимоги: а) бути унікальним чином пов'язаним із стороною, яка підписала документ, б) мати можливість ідентифікувати сторону, що підписала документ, с) створюватися з використанням засобів, які сторона, яка підписала документ, в змозі одноосібно контролювати; d) таким способом бути пов'язаним із даними, що дозволяє виявити подальшу в них зміну.

Слід зазначити, що згідно з п. 3 ст. 2 цієї Директиви під стороною, яка підписала документ, розуміється особа, у розпорядженні якої знаходиться пристрій зі створення електронних підписів, що діє від свого власного імені або від імені особи, що представляється ним (фізичної або юридичної). У свою чергу, пристрій зі створення електронних підписів є конфігурованим апаратним і програмним забезпеченням, що використовується для створення електронних підписів (п.5 ст.2 Директиви). З урахуванням технічно відкритого характеру «просунутого» електронного підпису та необов'язковості асиметричного способу шифрування Директива ЄС «Про загальні принципи електронних підписів» допускає можливість використання вільно доступних та поширених програм типу PGP або GnuPP. Так само, як і для простого електронного підпису, Директива не передбачає жодних інших правових наслідків використання «удосконаленого» електронного підпису, крім заборони дискримінації як доказу в процесі [194, с. 455].

Окремим питанням, що потребує уваги, виступає питання визнання іноземних сертифікатів електронних підписів. Відповідно до абз.1 ст.4 Директиви ЄС «Про загальні принципи електронних підписів» на держави у сфері дії Директиви покладається обов'язок не обмежувати сертифікати, видані сертифікованим сервісом – провайдером на території іншої держави – члена ЄС. Гарантія вільного поширення та переміщення на внутрішньому ринку встановлюється також для програмних продуктів для електронних підписів (абз.2 ст.4). Для сертифікатів із третіх держав ст.7 Директиви встановлює перелік вимог для визнання таких сертифікатів усередині ЄС. Перелік вимог детально прописаний тільки для кваліфікованих сертифікатів,

а порядок визнання «просунутих» електронних підписів з третіх держав Директива не встановлює, обмежуючись пропозицією для Європейського парламенту створити дійсні та ефективні правила у цій сфері [196, с.317].

Відповідно до абз.1 ст.7 Директиви держави-члени ЄС повинні гарантувати кваліфіковані сертифікати, видані сертифікуючим сервіс-провайдером, що діють у третій країні, які будуть визнаватись юридично еквівалентними сертифікатам, виданим сертифікуючим сервісом в рамках ЄС, за умови, що: а) сертифікуючий сервіс-провайдер, що діє у третій країні, відповідає вимогам, встановленим цією Директивою та має добровільну акредитацію в одній з держав - членів ЄС, або б) сертифікуючий сервіс-провайдер в межах ЄС, що відповідає вимогам Директиви, доручається за іноземний кваліфікований сертифікат, або с) кваліфікований сертифікат або діяльність сертифікуючого сервіс-провайдера, що діє в третій країні, визнані в рамках укладеної двосторонньої або багатосторонньої угоди між ЄС і третьою державою або міжнародною організацією [146, с.581].

Закон ФРН «Про цифрові підписи» був свого роду «першопрохідцем» у даній сфері на рівні країн ЄС. Однак до 2000 року Федеральний уряд Німеччини підготував доповідь «Про накопичений досвід та подальший розвиток у сфері комунікації та інформаційного законодавства» [88], в якому вказувалося на процес безперервного розвитку інфраструктури електронних підписів, при цьому було зазначено, що сам інститут електронного підпису як усередині самої Німеччини, так і в усьому світі знаходиться ще на початковому етапі свого розвитку [88]. Деякі положення доповіді, а саме питання регулювання відповідальності, і навіть можливості передачі функцій сертифікуючого сервіс - провайдера третій особі, увійшли до остаточного тексту нового Закону від 16.05.2001 «Про електронні підписи» [90, с.17; 234]. Необхідно відзначити, що цей Закон охоплює лише технічні вимоги, що пред'являються до електронного підпису, детальніше торкаючись тільки кваліфікованого електронного підпису.

Відповідно до § 25 Закону «Про електронні підписи» правове регулювання електронних підписів не обмежується рамками вищезазначеного закону, Федеральний уряд має право, згідно з п.1 § 25, шляхом прийняття розпоряджень Уряду, що мають силу закону (Rechtsverordnung), конкретизувати досить абстрактні положення зазначеного Закону. Розпорядження Федерального уряду «Про електронний підпис», що також носить технічний характер, набуло чинності 16.11.2001. Так, наприклад, цим Розпорядженням встановлюються стандарти перевірки програмних продуктів кваліфікованих електронних підписів (ISO/IEC 15408) і тд.

Законодавством Німеччини слідом за Директивою ЄС 1999/93/ЄС «Про загальні принципи електронних підписів» виділяються простий, «удосконалений» і кваліфікований електронний підпис. Визначення простого електронного підпису надане в п.1 § 2 Закону від 16.05.2001 «Про електронні підписи» дослівно повторює зазначене у п.1 ст.2 Директиви, а саме це дані в електронній формі, що додаються або логічно суміщені з іншими електронними даними та служать як метод розпізнавання. Слід зазначити, що порівняно з колишнім Законом 1997 року термін «цифровий підпис» було замінено терміном «електронний підпис». Цілями такої зміни послужили як гармонізація з європейським регулюванням, так і привнесення певної технологічної нейтральності в дане поняття [91, с.18]. Достатнім для простого електронного підпису, згідно з п.1 § 2 Закону від 16.05.2001 «Про електронні підписи», є або надруковане наприкінці ім'я автора, або відсканований особистий підпис. На думку німецького законодавця, ці вимоги не несуть у собі серйозної гарантії безпеки [91, с.18]. Втім, саме простий електронний підпис є найпоширенішим видом електронного підпису в електронному документообігу Німеччини [197].

Матеріально-правове значення простого електронного підпису полягає в тому, що згідно з § 126а Цивільного кодексу ФРН (далі – ЦК ФРН) він виконує вимоги, встановлені законом до форми тексту щодо волевиявлення

особи. Крім того, відповідно до абз.3 §127 ЦК ФРН у разі, якщо немає підстав вважати іншу волю сторін, то для дотримання встановленою угодою електронної форми (узгоджена форма) достатнім буде використання іншого електронного підпису, ніж кваліфікований. Процесуальне значення простого електронного підпису оцінюється судом із загальних позицій принципу вільної оцінки доказів у порядку передбаченому § 286 ЦПК ФРН та визначення його, згідно з абз.1 §371 ЦПК ФРН, як речового доказу.

Наступним видом електронного підпису, який виділяється Законом від 16.05.2001 «Про електронні підписи», є «удосконалений» електронний підпис. Відповідно до п.2 § 2 даного Закону до такого виду належать електронні підписи, які:

- унікальним чином пов'язані з власником сертифіката ключа підпису;
- дозволяють ідентифікувати власника сертифіката ключа підпису;
- створюються з використанням коштів, які власник сертифіката ключа підпису може одноосібно контролювати;
- таким способом пов'язаний із даними, що дозволяє виявити подальшу зміну.

Збільшення ролі торгівлі в мережі «Інтернет» викликає необхідність вирішення низки процесуальних проблем. Найважливіше значення при цьому приділяється правовому регулюванню зростаючої кількості документів, переданих в електронній формі. Поряд із цим, виникає питання про доказову силу таких документів. Особливого значення ця обставина набуває в разі, якщо, наприклад, договір укладається шляхом обміну повідомленнями електронної пошти. Вирішення цих питань нерозривно пов'язане з визначенням поняття електронного документа в праві Німеччини як родового поняття, з допустимістю та його доказовим значенням у цивільному процесі.

Починаючи з 1970-х років, в німецькій процесуальній літературі ведеться науковий спір із приводу визначення поняття машинний документ, його правове становище та про доказову силу даного документа [168]. Проте

аж до 2001 року ЦПК ФРН не містило спеціальних приписів про докази, що існують в електронній формі. З 2001 року в ЦПК ФРН було введено § 130a, в якому офіційно було зазначено допустимість у цивільному процесі електронних документів [224]. У цей період в абз.1 §371 ЦПК ФРН було вирішено питання про віднесення електронного документа до речових доказів. З набранням чинності 22.03.2005 Закону «Про використання електронних форм комунікації у судочинстві» (Gesetz über die Verwendung elektronischer Kommunikationsmittel in der Justiz¹ [159]) деякі норми ЦПК ФРН було викладено в новій редакції, а також було введено § 371a, який поширювався на приватні електронні документи, що мають кваліфікований електронний підпис, правила про доказову силу приватних документів (письмових доказів). До електронних документів, складених в установленій формі органом публічної влади в межах його компетенції (офіційним електронним документам), згідно з абз.2 §371a ЦПК ФРН застосовуються правила про доказову силу офіційних документів (письмових доказів).

Слід зазначити, що ні зазначена норма, ні інші приписи ЦПК ФРН не містять легального визначення поняття «електронний документ», вказуючи лише на окремі його ознаки. Так, зі змісту §130a ЦПК ФРН випливає, що електронний документ є «здатним бути прочитаним та обробленим записом» будь-якої заяви, клопотання, інших процесуальних документів. У рамках цивільного судочинства ця норма надає сторонам можливість представляти суду в електронній формі підготовчі документи та клопотання [163]. Законом «Про використання електронних форм комунікації в судочинстві» з прийняттям §130b було додатково запроваджено поняття «судовий електронний документ». У той час, як регулюванням §130a охоплюються електронні документи сторін та інших учасників процесу, положення §130b стосуються документів, що вимагають власноручного підпису від судді, співробітника судової служби, службовця канцелярії суду або від судового виконавця (судове рішення, ухвала, розпорядження), до яких прирівнюється запис у формі електронного документа із проставленням наприкінці

документа імені посадової особи та кваліфікованого електронного підпису. Слід зазначити, що §130b не замінює письмову форму таких документів шляхом введення електронної форми, а встановлює взаємозамінність власноручного підпису та кваліфікованого електронного підпису з проставленням імені посадової особи в кінці документа.

Виходячи з контексту, абз.1 § 371 ЦПК ФРН в німецькій процесуальній літературі під електронним документом прийнято розуміти текстові, аудіо, - відео- та програмні документи [234]. Така думка ґрунтується на віднесенні електронного документа до речових доказів, і, відповідно, розумінні його як файлу, який може бути записаний на носії інформації [182]. Відповідно до цієї концепції необхідно чітко відмежовувати файл від електронного документа, оскільки останній може бути в тимчасовій (оперативній) пам'яті комп'ютера. На відміну від цього, файл завжди передбачає постійне зберігання на жорсткому диску комп'ютера. Крім того, електронний документ може бути збережений у вигляді файлу, який у цьому випадку виступає в ролі середовища зберігання документа.

Таким чином, формулювання абз.1 § 371 ЦПК ФРН виходить із широкого розуміння електронного документа. Поняття електронного документа в цьому контексті охоплює вже не тільки заяви, клопотання, інші процесуальні документи в електронній формі, а також незалежно від їх змісту графічні, аудіо- та відеофайли. Важливою ознакою тут виступатиме можливість збереження документа у вигляді файлу на носії інформації, оскільки згідно з зазначеним приписом йдеться про вид речового доказу [220].

На відміну від зазначеного формулювання, § 371a ЦПК ФРН виходить із вузького розуміння електронного документа, який є заявою в електронній формі. До них можуть належати нагадування про сплату боргу, квитанції. Багато в чому зміни у ЦПК ФРН та чинні редакції параграфів несуть на собі відбиток попередньої дискусії у процесуальній літературі. Так, питання про віднесення електронного документа до певного виду доказів інтенсивно

дискутувалося до 2001 року, до набуття чинності нової редакції §371 ЦПК ФРН, який однозначно вирішив питання речових доказів. Однак, через відсутність легального визначення електронного документа, нині в літературі існують різні точки зору з цього питання.

Відповідно до підходу Арнда Беккера під електронним документом розуміється будь-яка можлива довготривала фіксація відомостей на носії інформації при використанні електронного перетворення сигналу. Електронний документ - це насамперед комп'ютерний файл, який створюється, зберігається і пересилається з використанням програмного забезпечення [80]. Словосполучення «фіксація відомостей» використовується автором підходу для відмежування поняття електронного документа від заяв в усній формі. Формулювання «використання електронного перетворення сигналу» служить цілям відмежувати електронний документ від документів, виготовлених за допомогою друкарської машинки або виконаних від руки. При цьому, згідно з цим підходом, під носії інформації в зазначеному визначенні підпадають як електронні носії (дискети, CD-ROM), так і інші носії, у тому числі паперові, на яких роздруковується електронний документ. У цьому випадку йдеться про репродукцію електронного документа (роздруківки), яка згідно з цією точкою зору є також електронним документом. Таким чином, з поняття електронного документа виключаються лише письмові документи, виконані від руки або з використанням друкарської машинки. Такий підхід, у свою чергу, веде до проблеми відмежування від поняття письмових документів у ЦПК ФРН.

У літературі у зв'язку з цим зазначається, що положення про доказову силу письмових документів § 415 та абз.2 § 440 ЦПК ФРН відносяться виключно до документів, підписаних від руки або засвідчених нотаріально [234]. Такі види документів, як комп'ютерний факс, роздрук електронного документа, телефакс, відносяться також до письмових документів у сенсі ЦПК ФРН [80, с. 127]. Щодо копій такого виду письмових документів, як

телефакс, у процесуальній літературі вироблено підхід, згідно з яким ці копії є письмовим документом та доказом у суді лише в разі втрати оригіналу.

Слід зазначити, що в науці сформувався однозначний підхід до файлу електронного документа: цей файл не є письмовим доказом у сенсі ЦПК ФРН, оскільки відсутні такі елементи письмового документа як докази: а) письмовий характер (*Schriftlichkeit*) та б) оборотоспроможність (*Verkehrsfähigkeit*) [68].

Згідно з іншою точкою зору [85], що ґрунтується на формулюванні § 126а ЦПК ФРН, під електронним документом слід розуміти будь-які відомості в електронній формі, зміст яких може бути прочитаний із використанням письмових знаків. Крім цього, ще однією важливою вимогою до електронного документа, згідно з цим підходом, є збереження документа в такий спосіб, який дозволяє багаторазово й довгостроково мати доступ до документа [85]. Ця вимога вважається виконаною, коли волевиявлення зафіксовано таким способом, що його укладач втрачає можливість змінювати щось, а видалення знаходиться виключно у сфері його отримувача. Відповідно до § 126а ЦПК ФРН необхідними вимогами також виступають доповнення волевиявлення своїм ім'ям та постачання електронного документа кваліфікованим електронним підписом. При аналізі цієї точки зору привертає увагу обмеження поняття «електронний документ» на відомостях, зміст яких може бути прочитано з використанням письмових знаків. У зв'язку з цим автоматично виключаються з такого визначення, а отже, з тлумачення пред.2 абз. 1 § 371 ЦПК ФРН аудіо- та відеофайли. У той же час перевагою даного підходу є наявність чітко сформульованих вимог до електронного документа з посиланням на матеріальне право, виходячи з яких, формулюються також і деякі норми про докази в ЦПК ФРН.

Узагальнюючи вищесказане, слід зазначити, що дві представлені та існуючі в літературі точки зору торкаються різних аспектів поняття «електронний документ» і один одному не суперечать. Автор першого підходу намагався об'єднати в поняття «електронний документ» якнайбільше

видів та форм документів. У свою чергу, другий підхід зупиняється на виділенні окремих, важливих з правової точки зору аспектів електронного документа. У цій роботі використовується друга точка зору, яка найбільш детально відображає це поняття та вимоги до електронного документа як доказу в суді.

Під письмовими доказами в цивільному процесі Німеччини традиційно розуміється письмово виражена за допомогою певних знаків думка, для розуміння якої потрібні спеціальні засоби. Письмові докази вважаються дуже достовірними доказами з високою доказовою силою. У процесуальній науці Німеччини були сформульовані такі основні ознаки письмових доказів, як: наявність думки (*Gedankenerklärung*), вираз/втілення (*Verkörperung*), безпосереднє сприйняття (*unmittelbare Wahrnehmbarkeit*). Наявність думки, на думку більшості німецьких процесуалістів, є основною відмінною ознакою письмового доказу [87].

У деяких випадках додається, що мова повинна йти тільки про «первинні» людські думки [234]. У цьому сенсі масив даних електронного документа не містить «первинних» людських думок, а являє собою винятково факт введення конкретного програмного коду [80].

Наступною ознакою письмового доказу є вираз думки, що означає фіксацію сформульованої думки на носії шляхом використання певних знаків (літер та цифр). У питанні про наявність цієї ознаки письмового доказу електронний документ у літературі не має єдності думок. Відповідно до одного підходу дію цієї ознаки можна поширити на паперові носії, комп'ютерні жорсткі диски, дискети, CD-ROM, аудіо- та відеозаписи. Автори іншої точки зору вважають, що електронний документ не має довгострокового вираження/фіксації думки. Як обґрунтування наводиться аргумент, що електронний документ неминуче змінює носій інформації, на відміну традиційного письмового документа, який завжди залишається на тому ж носії. При цьому зазначається, що виведення на монітор комп'ютера електронного документа, незважаючи на наявність у ньому букв і цифр, не

охоплюється цією ознакою через відсутність довготривалості та незмінності. Такий документ є швидкоплинним і може бути прочитаний рівно стільки, скільки буде увімкнено комп'ютер в електричну мережу. В разі збереження електронного документа на носії (напр. CD-ROM) проблема довгостроковості та незмінності вмісту зникає, проте в цьому випадку буде відсутнє письмове вираження думки та її «первинність». З цих причин така ознака письмового доказу, як вираз думки, у випадку з електронним документом відсутня.

Традиційно заключною ознакою письмового доказу в цивільному процесі Німеччини є безпосереднє сприйняття. Згідно з панівною в літературі точкою зору письмове підтвердження в сенсі § 415 і наступних ЦПК ФРН є таким, тільки якщо існує можливість його безпосереднього сприйняття [179]. Таке сприйняття, у свою чергу, означає неприпустимість використання технічних засобів перетворення в письмові знаки (літери, цифри). У цьому сенсі електронний документ без необхідного програмного та апаратного забезпечення не читається, а отже, не може безпосередньо бути сприйнятий, оскільки складається тільки з нулів та одиниць (двійкового коду). З огляду на дані якості електронного документа він виключається зі сфери дії §415 ЦПК ФРН.

Виходячи з вищевикладеного, можна зробити висновок, що електронний документ не є письмовим доказом у цивільному процесі Німеччини в традиційному його розумінні. Крім того, згідно з панівною в науковій літературі позиції, використання кваліфікованого електронного підпису в порядку, визначеному § 2 №3 Закону «Про електронні підписи», в електронному документі розглядається як несуттєва обставина з погляду правового статусу електронного документа у доказовому праві [199]. Так само й новий §371a ЦПК ФРН, введений Законом «Про використання електронних форм комунікації в судочинстві» (Justizkommunikationsgesetz), згідно з положеннями якого, до приватних електронних документів, що мають кваліфікований електронний підпис, застосовуються правила про

доказову силу приватних документів (тобто правила про доказову силу письмових доказів), не вплинули на положення електронного документа як речового доказу.

З моменту набуття чинності Законом від 12.07.2001 «Про адаптацію встановленої процесуальної форми» (Formvorschriftenanpassungsgesetz) було змінено редакцію пред.2 абз.1 § 371 ЦПК ФРН, яка за задумом законодавця повинна була поставити крапку в дискусії з питання кваліфікації електронного документа як доказу, а саме вирішити питання на користь речового доказу. Речові докази в теорії цивільного процесу Німеччини мають бути досліджені судом шляхом безпосереднього сприйняття і переконання у правильності тих чи інших спірних фактів [234]. На відміну від письмових доказів, у даному випадку йдеться не про пізнання думки, викладеної в документі, а про безпосереднє (реальне) пізнання речі або людини з точки зору їх існування та властивостей. При оцінці речових доказів, до яких відносяться також і електронні документи, діє принцип вільної оцінки доказів (§ 286 ЦПК ФРН). Відсутність винятків з цього принципу, як у випадку з письмовими доказами, обґрунтовується тим, що в більшості випадків електронні документи є графічними або текстовими файлами, які досить легко можуть бути змінені, що, у свою чергу відбивається на достовірності електронного документа як доказу [103] .

У німецькій процесуальній літературі існує дискусія про те, що саме вважати об'єктом дослідження електронного документа як речового доказу. Деякі автори називають таким об'єктом сам електронний документ [136], інші – його електронним носієм [199]. Слід зазначити, що, зазвичай, електронний документ, саме комп'ютерний файл, його зміст, виступають об'єктом судового дослідження. У той же час не можна виключати, що електронний носій, наприклад, жорсткий диск комп'ютера або CD-ROM, може виступати в цій якості. Визначальним чинником тут можуть бути позиції сторін у процесі. Так, якщо питання ставиться про певний зміст електронного документа (наприклад, повідомлення електронної пошти),

об'єктом є сам електронний документ. У випадку, коли йдеться про існування електронного файлу (наприклад, той факт, що повідомлення електронної пошти було доставлене та збережене в поштовій скриньці), об'єктом дослідження в суді може бути електронний носій (наприклад, поштовий сервер).

У цивільному процесі Німеччини загальні вимоги, що пред'являються до речових доказів, прийнято застосовувати й до електронних документів. Поруч із, судовою практикою було виділено приклади недопустимих речових доказів. До таких відносяться прихований аудіозапис, фотографування та відеозапис особи без отримання її згоди. Слід зазначити, що неприпустимість доказу в німецькому цивільному процесі розуміється виключно відхиленням доказу за наявності підстави недопущення доказу, зазначеного в законі (Beweisverbot), а отже, вирішення питання про прийняття чи відхилення доказу, внаслідок його неприпустимості, не перебуває в компетенції суду.

У теорії цивільного процесу Німеччини до речових доказів було висунуто дві основні вимоги: ідентичність (Identität) і нефальсифікованість (Unverfälschtheit) [86]. Ідентичність доказу означає, що поданий доказ підтверджує (своїм існуванням, змістом, властивостями) саме ті обставини, на які посилається сторона, що представила цей доказ. Документ вважається ідентичним, якщо однозначно можна встановити його укладача, а сам укладач може бути ідентифікований. Стосовно електронного документа, вимога ідентичності передбачає, що поданий/переданий суду електронний документ є ідентичним тому, який був пересланий протилежною стороною.

Поряд з ідентичністю електронного документа теоретично прийнято виділяти також ідентичність електронного носія документа. Даний вид ідентичності має важливе значення в тих випадках, коли необхідно довести використання конкретною особою конкретного електронного носія інформації. Насамперед, питання ідентичності електронного носія виникає у справах про порушення авторських прав у мережі «Інтернет». У цих випадках важливим із точки зору доказування є те, що певний носій

інформації (наприклад жорсткий диск домашнього комп'ютера) користувача соціальних обмінних мереж типу BitTorrent або eMule використовується для зберігання незаконно завантажених фільмів або музики.

Під нефальсифікованістю електронного документа теоретично розуміється припущення в тому, що конкретний файл було отримано користувачем. Ця вимога обґрунтовується тим, що або під час пересилання файлу, або в той час, коли файл вже знаходиться в системі одержувача, існує велика ймовірність його фальшування.

На практиці щодо електронного документа йдеться про те, що певне волевиявлення (наприклад, оферта електронною поштою) було доставлено на поштову скриньку одержувача. Як правило, повідомлення електронної пошти під час пересилки з комп'ютера відправника проходить безліч проміжних станцій до моменту доставки одержувачу. Момент доставки повідомлення електронної пошти пов'язаний із певними труднощами в доведенні ще й тому, що ні відправник, ні одержувач не мають жодного впливу на те, яким чином (через які проміжні станції/сервери тощо) буде здійснено доставку, а також те, коли саме повідомлення буде доставлено.

Проте слід зазначити, що судовою практикою вироблено підхід, згідно з яким доведення справжності самого електронного документа в разі його заперечення в процесі саме по собі не буде достатнім [172, с.55]. Ця позиція ґрунтується на тому положенні, що ідентичність і нефальсифікованість електронного документа не є повною гарантією його справжності, оскільки він легко може бути змінений. У цьому випадку такою гарантією може виступати електронний підпис. Відповідно до абз.1 § 371а ЦПК ФРН електронний документ, що має кваліфікований електронний підпис, має ту саму доказову силу, що й приватні документи, залишаючись при цьому речовим доказом. При дотриманні вимог, встановлених абз.1 § 371а ЦПК ФРН, електронний документ (речовий доказ) є повним доказом справжності заяви. При цьому засноване на результаті перевірки електронного підпису припущення про справжність заяви, що існує в електронній формі, згідно з

п.2 абз.1 § 371a, може бути оскаржене лише фактами, які обґрунтовують серйозні сумніви в тому, що заява зроблена власником електронного підпису. Справжність заяви в електронній формі з кваліфікованим електронним підписом також охоплює вищезазначені загальні вимоги до електронного документа як до речового доказу, а саме нефальсифікованість заяви та належність заяви власнику електронного підпису – ідентичність [198, с.807]. Крім цього, використання кваліфікованого електронного підпису в порядку, передбаченому п.3 §2 Закону «Про електронні підписи», дозволяє забезпечити досить високий рівень гарантій ідентичності та нефальсифікованості електронного документа. Високий рівень забезпечується за рахунок використання в алгоритмі роботи електронного підпису хеш-функції, яка дозволяє швидко та легко встановити, чи вносилися до електронного документа зміни після його виготовлення, однак із змісту названого параграфу можна зробити висновок, що використання кваліфікованого електронного підпису є не єдиною вимогою, встановленою § 371a ЦПК ФРН. Особливою вимогою виступає подання заяви в електронній формі. Зазначені вимоги сформульовані в § 126a Німецького цивільного укладення. Згідно з цим положенням, заява вважається поданою в електронній формі, якщо файл збережений за допомогою електронного носія і може бути прочитаний тільки за допомогою спеціальних технічних засобів [88, с.25].

Крім цих двох вимог, у літературі вказується на необхідність можливості виведення заяви на екран комп'ютера у вигляді письмових знаків, як додаткова вимога [209].

Крім двох вищеперелічених, протилежних один одному точок зору, в німецькій процесуальній літературі зустрічається проміжна позиція стосовно доказової сили повідомлень електронної пошти. Відповідно до цього підходу необхідно відмежовувати доказове значення простого незахищеного повідомлення електронної пошти від волевиявлень - повідомлень, переданих через захищений протокол на певній інтернет-платформі [123]. У свою чергу,

в простих незахищених повідомленнях важливо розділяти в процесі доведення належність адреси електронної пошти конкретній особі та належність надісланого повідомлення власнику адреси електронної пошти. Перша альтернатива стосується питання про те, чи належить, наприклад, адреса електронної пошти moskovchuk@gmail.com особі на прізвище Московчук. Важливо відзначити, що в більшості провайдерів електронної пошти під час реєстрації адреси електронної пошти (поштової скриньки) повністю відсутня процедура ідентифікації користувача. Виходячи з цього, буде правомірним заперечення доказової сили повідомлень електронної пошти з точки зору ідентифікації особи, яка володіє адресою електронної пошти. Втім, практично перша альтернатива зустрічається досить рідко. Набагато актуальнішим є питання про те, що повідомлення електронної пошти із зазначеним відправником moskovchuk@gmail.com було справді надіслано власником цієї адреси електронної пошти. На сьогодні надіслати повідомлення з електронної пошти, використовуючи чужу адресу, не є чимось складним із технічної точки зору й доступне пересічному користувачеві. Крім того, використовуючи додаток «telnet», що входить у стандартний набір програм операційної системи сімейства «Microsoft Windows», та виконуючи покрокову інструкцію, розміщену у вільному доступі в мережі «Інтернет», можна надіслати повідомлення з електронної пошти, використовуючи будь-яку вигадану/реальну адресу електронної пошти.

Виходячи з викладеного, слід зазначити, що через ненадійність гарантії приналежності відправленого повідомлення власнику адреси електронної пошти доказова сила речового доказу з погляду вимоги ідентичності в таких повідомлень відсутня. У порівнянні з панівною точкою зору, відмінність даного підходу полягає в тому, що повідомлення, надіслані через захищений протокол на певній інтернет-платформі (напр. популярний інтернет-магазин «e-bay»), відповідають вимогам ідентичності речових доказів. Принципова відмінність полягає в тому, що з процесуальної точки зору, тут виникає

додатковий учасник процесу - власник інтернет-платформи. Вступ даного учасника покликаний обмежити втручання третіх осіб, а за наявності такого - шляхом подання відомостей власником інтернет-платформи в порядку, передбаченому § 142, 144 ЦПК ФРН, розкрити інформацію про те, ким і коли воно було створено.

3.3. Принцип еквівалентності паперових та електронних документів у законодавстві Італійської Республіки

Італія була однією з перших країн у світі, яка прирівняла юридичну силу електронного документа, підписаного за допомогою цифрового підпису, до документів, написаних і підписаних на паперових носіях. Стаття 15 § 2 Закону 59/19971 [170] запровадила основний принцип еквівалентності паперових та електронних документів: акти, дані та документи, складені державою та фізичними особами за допомогою електронних засобів, договори, укладені в тій самій формі, а також їх зберігання та передача електронними засобами є дійсними та відповідними для всіх намірів та цілей закону.

Цей закон дозволив використовувати інформаційні технології для підвищення ефективності й державного управління, і судового доказування, але його впровадження відбувалося дуже повільно [206].

Законодавча позиція контролюється Кодексом цифрового адміністрування (Кодекс цифрового управління), введеним у законодавство декретом 82/2005 [107]. КЦУ має на меті забезпечити систематичне регулювання обміну цифровою інформацією між державними адміністраціями; зберігання електронних документів; створення національної мережі електронних документів та підписів. Закон N. 229/20035 [171] встановлює керівні принципи для правил КЦУ і визначає цілі наступним

чином: «... забезпечити якнайширшу доступність інформаційних послуг урядами та іншими державними установами та гарантувати громадянам та підприємствам доступ до таких послуг відповідно до максимального спрощення інструментів і процедур, з дотриманням принципів рівності та недискримінації та відповідно до нормативних актів про конфіденційність персональних даних».

Однак, менш ніж за десять років до КЦУ було внесено кілька поправок. Ці постійні зміни сприяли невизначеності, перешкоджаючи використанню процедури відмови та перевірки електронних підписів, та затримуючи еволюцію судової практики цієї спрямованості.

Протягом двадцяти років набули чинності низка змін до нормативних положень, які продемонстрували очевидну невизначеність італійського законодавця в роботі з термінами, визначеними інформаційними технологіями з самого початку [115, с.835].

На початку Указ Президента № 513/199710 [104] встановив «критерії та умови впровадження» еквівалентності між електронним документом, підписаним цифровим підписом, і документом із власноручним підписом. Для цього стаття 5 надає електронному підпису таку ж ефективність, як це передбачено ст. 2702 Цивільного кодексу Італії для власноручного підпису [105]. Постанова 1997 року згодом була замінена Указом Президента № 445/2000 [113, с.12], який привів правила, що регулюють електронні документи, у відповідність із законодавством щодо цифрового підпису без втрати узгодженості нової системи, заснованої на повній еквівалентності цифрового підпису рукописному підпису.

Директива ЄС була також причиною зміни італійського законодавства. Директива була спрямована на полегшення використання електронних підписів і сприяла їх юридичному визнанню в країнах-членах Європейського Союзу. З цією метою положення Директиви ґрунтуються на принципі технологічної нейтральності, який забороняє національному законодавству впливати – навіть опосередковано, з посиланням на технічні стандарти,

прийняті для конкретних продуктів, – на вільний рух товарів і послуг, які можна використовувати для електронних підписів [216, с.183].

В Італії законодавство, яке застосовувалося до прийняття Директиви, стосувалося виключно шифрування з відкритим ключем. Це означало, що необхідно розпізнавати інші форми електронного підпису, такі як комбінації даних (особистий ідентифікатор, пов'язаний з паролем, який використовується для отримання доступу до комп'ютерних систем); введення імені в електронний документ; персональний ідентифікаційний номер (PIN-код); ім'я в адресі електронної пошти та підпис рукопису, який був відсканований, серед іншого.

2 березня 2002 року Законодавчий декрет № 10/2002 набрав чинності [106]. Цей указ транспонував положення Директиви та замінив статтю 10 Указу Президента № 445/2000, що свідчить про значні зміни в регулюванні електронного підпису [165]. Зокрема, переглянута стаття 10L залишалася в силі до 31 грудня 2005 року і як наслідок, таким документам було присвоєно більшу доказову ефективність, ніж документ, написаний і підписаний на папері [111]. Отже, це правило піддалося жорсткій критиці науковцями, оскільки воно не передбачало ідеї повної еквівалентності, як це нав'язує Директива [195].

Кодекс цифрового адміністрування [127] переглянув законодавство відповідно до принципу та вказівок, визначених Законом № 1.229 від 2003 року [171].

Правила щодо електронних документів та електронного підпису були об'єднані в текст КЦУ, який набув чинності 1 січня 2006 року. Метою було забезпечити правову основу для їх використання громадськістю в управлінні та між громадянами та бізнесом.

Проте можна виявити деякі явні невідповідності: по-перше, запровадження чотирьох видів електронного підпису. До «електронного підпису» та «розширеного електронного підпису» (незрозуміло) додаються «кваліфікований електронний підпис» і «цифровий підпис». Перший додав

«кваліфікований сертифікат» до визначення «розширеного підпису», запропонованого Директивою ЄС; останнє характеризується «системою криптографічних ключів, один відкритий і один приватний, пов'язаних один з одним».

Крім того, через кілька місяців після набрання ним чинності Законодавчим декретом №159 від 2006 р. додано цілий розділ, присвячений публічним мережам, а статті 20 і 21, присвячені принципівому питанню доказової сили електронного документа, переписані. Зміни до останніх положень розширили вільну оцінку суду на цілісність та незмінність, а також якість та безпеку електронних документів, підписаних електронним підписом (ст. 21 § 1), та ввели «презумпцію підпису» (ст. 21 §2), яка спричинила серйозні наслідки щодо перевірки підпису: «Передбачається, що особа, яка має підписний пристрій, є особою, яка проставляє підпис, якщо вона не доведе інше»

Згодом стаття 14 Законодавчого декрету № 235 від 2010 р. [108] замінила заголовок статті 21 КЦУ в *Documento informatico sottoscritto con firma elettronica* (Електронний документ, підписаний електронним підписом) та внесла зміни до пункту 2 статті 21, розширюючи дію статті 2702 ЦК Італії, яка раніше використовувалась лише в разі використання цифрового або кваліфікованого електронного підпису, на будь-який «електронний документ, підписаний на розширений, цифровий або кваліфікований електронний підпис, «[...] що забезпечує ідентифікацію автора, цілісність і незмінність документа».

Крім того, статтею 14 Законодавчого декрету № 235 від 2010 року до статті 21 додано пункт 2-б, у якому чітко визначено, які електронні документи відповідають вимогам письмової форми, передбаченим статтею 1350 ЦК Італії, а саме: «за винятком випадків, передбачених статтею 25, приватні листи, зазначені в статті 1350, частинах першого абзацу від 1 до 12 Цивільного кодексу, якщо вони зроблені за допомогою комп'ютерного

документа, підписуються кваліфікованим електронним підписом або з цифровим підписом».

У законі № 221 від 2012 року [169] знову викладено детальні положення щодо юридичної цінності та доказової ефективності електронних документів. Ці зміни внесли додаткові зміни до чинного положення.

Визначення електронного документа, викладене в статті 1(p) КЦУ «documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti» «комп'ютерний документ: інформаційне відображення дій, фактів або юридично релевантних даних». Можливо, це визначення недостатньо детальне, проте з деякими корективами воно посиляється на традиційне визначення документа прийнятого Цивільним кодексом Італії [226]. Однак, для належного вивчення теми необхідно розглядати електронний документ як документ, що містить цифрові дані, для існування якого необхідне обладнання та програмне забезпечення [215].

Всупереч тому, що уявляють деякі вчені [188], електронний документ (точніше, дані в цифровому форматі) потребують матеріального забезпечення. У той час як традиційний документ записується на папері, електронний документ зберігається на різних типах обладнання, доступних в альтернативних форматах, таких як магнітні диски (диски), оптичні диски (CD-ROM - DVD-ROM) і жорсткі диски.

Щоб забезпечити та зберегти свідчення факту (наприклад, оплата зобов'язання) або сформувані відповідний акт (наприклад, заяву чи договір), документ завжди буде зберігатися на апаратному забезпеченні – тобто фізичному елементі – носії, на якому записані дані [185]. Незалежно від носія, на якому записаний документ, а також від його декларативної чи розповідної функції, документ повинен мати можливість зберігатися за допомогою зрозумілих знаків і таким чином, щоб він не був змінений.

Що стосується електронного документа, то дані зберігаються за допомогою двійкового коду. Ця послідовність бітів була б швидкоплинною та нечитабельною без програмного забезпечення, здатного представляти

текст у формі, доступній для читання, тому електронний документ — це набір цифрових даних, записаних у формі, яка може бути прочитана програмним забезпеченням, для інформаційного представлення дій, фактів або юридично релевантних даних» [114].

Можна розрізнити «відтворення» та «записи» з посиланням на електронні документи. Інформаційне відтворення документа, що відображає факт, охоплюється статтею 2712 ЦК Італії під назвою «Механічні відтворення» («Riproduzioni meccaniche»), яка передбачає наступне.

Фотографічні або кінематографічні репродукції, фонографічні реєстрації та, загалом, механічне відтворення фактів або речей є повним доказом представлених фактів і речей, якщо особа, якою вони створені, не відмовляється від своєї згоди з тими ж фактами та речами.

Інформаційне відтворення є електронним документом без підпису, і його придатність для задоволення вимоги письмової форми та його доказова сила вільно оцінюється суддею з огляду на його об'єктивні характеристики якості, безпеки, цілісності та незмінності, як зазначено у статті 20 § 1 b КЦУ.

Придатність електронного документа задовольняти вимозі письмової форми та його доказову силу можна вільно оцінити в суді з огляду на його об'єктивні характеристики якості, безпеки, цілісності та незмінності, без шкоди для положень статті 21 КЦУ.

Навпаки, існують документи, створені в цифровому вигляді, які називаються «інформаційними записами», які формуються за допомогою програмного та апаратного забезпечення та відображаються на екрані або на папері при роздрукуванні, де тип електронного підпису впливає на юридичну цінність і доказову цінність ефективність документа.

Чотири різні електронні підписи, визначені КЦУ, по суті відносяться до двох загальних категорій, описаних у статті 2 Директиви ЄС: електронний підпис, призначений як «дані, об'єднані з іншими даними», і розширений електронний підпис, призначений як «дані, пов'язані з документом». Дійсно, кваліфіковані електронні підписи та цифрові підписи відповідають вимогам

«простежуваності» та «виключного контролю» пристрою підпису та «незмінності» даних, які пов'язані з удосконаленням електронним підписом. Однак для них характерна потреба в кваліфікованому сертифікаті або системі криптографічних ключів.

Електронний підпис - набір даних в електронній формі, доданих або логічно пов'язаних з іншими електронними даними, що використовуються як спосіб ідентифікації. Тому, відповідно до цього визначення, електронний підпис використовується для індикативної функції, а не лише для підпису податкової декларації.

Прикладом є PIN-код дебетової та кредитної картки. До апарату, зазвичай банкомату, пред'являється картка. Картка може бути у клієнта банку, або карта може бути у володінні іншої особи, яка була отримана від фактичного клієнта, або злодій може вставити підроблену картку. Програмне забезпечення в банкоматі взаємодіє з програмним забезпеченням на картці. Програмне забезпечення має на меті ідентифікувати, що було введено правильний PIN-код. PIN-код є доказом того, що банк пропустив клієнта й правильна картка присутня для надання послуги [129].

Так само ім'я користувача та пароль, які використовуються користувачем для ідентифікації постачальника послуг електронної пошти, також мають індикативну функцію. Стверджується, що існує сумнівна судова практика щодо цього питання [211]. Італійські суди неодноразово постановляли, що непідписане повідомлення електронної пошти може становити електронний документ, підписаний електронним підписом [128]. Цей аналіз йде від ідеї, що відправник, щоб створити та надіслати електронний лист, повинен виконати дію підтвердження шляхом введення його особистої ідентифікації (ім'я користувача) та пароля його коду доступу. Можна стверджувати, що ідентифікаційні коди, використані як підпис автора, мають надсилатися одержувачу повідомлення [178].

Розширений електронний підпис визначається статтею 1(qbis) КЦУ таким чином: «розширений електронний підпис: набір даних в електронній

формі, доданий до електронного документа або пов'язаний із ним, що дозволяє ідентифікувати підписувача документа та забезпечує унікальний зв'язок із підписантом, створений за допомогою засобів, які підписувач може підтримувати під своїм виключним контролем, пов'язаний із даними, до яких відноситься цей знак, таким чином, щоб визначити, чи були дані згодом змінені»

Науковці схильні кваліфікувати графометричний підпис [166], нанесений стилусом на електронному планшеті, як приклад розширеного електронного підпису [70]. Програмне забезпечення фіксує поведінкові біометричні особливості автора [134] (такі як швидкість, точність, кут нахилу, прискорення і кількість разів, коли ручка піднімається з поверхні для письма). Програмне забезпечення перетворює біометричні дані, записані в цифровому вигляді, у зображення підпису, яке можна читати, і порівнює дані з даними, отриманими від попередніх підписів тією ж особою [118].

Цей метод набуває широкого поширення, особливо в банківському секторі, через можливість збору біометричних даних, коли клієнт розписується за допомогою традиційного жесту підпису. Біометричні дані, зібрані під час підписки, будуть зашифровані за допомогою відкритого ключа, виданого органом із сертифікації та нанесеного на документ у вигляді електронного підпису. Справді, підписку на планшеті також можна використовувати лише для цілей ідентифікації, щоб отримати доступ до послуги або поєднуватися з іншими електронними підписами.

Більше того, ніщо не перешкоджає використанню біометричних даних, зібраних під час підписки, для генерації приватного ключа, який, коли він пов'язаний із відкритим ключем, що охороняється сертифікатором, дозволяє наносити цифровий підпис на документ. Шифрування тексту за допомогою біометричних даних і додавання кваліфікованого сертифіката здається досяжним за допомогою криптографічної системи асиметричних ключів, заснованих на використанні руки.

Навряд чи можна знайти приклад кваліфікованого електронного підпису, який, у свою чергу, визначений статтею 1(r) КЦУ як: «кваліфікований електронний підпис: особливий тип розширеного електронного підпису, заснований на кваліфікованому сертифікаті та створений захищеним пристроєм для створення підпису».

Загальна думка вчених полягає в тому, що кваліфікований електронний підпис не можна відрізнити від цифрового, оскільки можна використовувати лише технологію, яка базується на шифруванні асиметричним ключем [73, с.500].

Різницю можна проаналізувати, посилаючись на програми, які використовуються для віддаленого керування банківською діяльністю [232]. Деякі банки надають своїм клієнтам пристрій, який генерує псевдовипадковий числовий код, який називається маркером. Номер синхронізується з сервером аутентифікації під контролем банку, який генерує той самий псевдовипадковий код. У цій схемі «безпечний» канал, по якому код передається від клієнта до банку, створюється шляхом шифрування повідомлення відкритим ключем, згенерованим одержувачем (банком). Після цього повідомлення буде розшифровано за допомогою приватного ключа, який створив банк і залишився під його контролем. Після закінчення операції пара ключів буде видалена.

Четвертий підпис - це цифровий підпис, визначений статтею 1(a) КЦУ таким чином: «цифровий підпис: особливий вид розширеного електронного підпису, заснованого на кваліфікованому сертифікаті та системі криптографічних ключів, один відкритий і один приватний, пов'язаних один з одним, що дозволяє власнику, використовуючи закритий ключ, і одержувачу, використовувати закритий ключ відповідно, щоб показати та перевірити походження та цілісність електронного документа або набору електронних документів».

Іншими словами, найстаріший і найпоширеніший розширений цифровий підпис складається із застосування послідовності літеро-цифрових

символів до електронного документа, які отримують шляхом вилучення з тексту репрезентативного зразка ("хеш-значення" або "збірка повідомлення") і шифруються за допомогою «приватного» ключа, як частини криптографічної системи асиметричних ключів [72].

КЦУ вимагає, щоб криптографічна система ключів була заснована на сертифікаті, виданому кваліфікованим сертифікатором, і щоб підпис «створено за допомогою інструментів, які підписувач може підтримувати під виключним контролем».

Як зазначалося раніше, електронний підпис впливає на правову та доказову цінність електронного документа. Відповідно до положень статей 20 і 21 усі електронні документи, навіть якщо вони не підписані, є ефективними за своїми об'єктивними характеристиками якості, безпеки, цілісності та незмінності. Однак вільне оцінювання судді виключається наявністю розширеного, цифрового або кваліфікованого електронного підпису.

Щодо значення в законі необхідно виділити наступне:

1. Лист, передбачений пп. 1-12 ст. 1350 ЦК Італії, в яких вимога письмової форми задовольняється електронним документом, підписаним кваліфікованим електронним або цифровим підписом (ст. 21 § 2/bis КЦУ).

2. Інші документи, які потребують письмової форми, передбачені п.п. 13 ст.1350 ЦК, повинні бути підписані розширеним, цифровим або кваліфікованим електронним підписом (стаття 21 § 2/bis КЦУ).

3. Усі інші письмові документи, в яких письмова форма потрібна лише для доказових цілей, можуть бути підписані будь-якою формою електронного підпису [77].

Після внесення змін до статті 21 Законом № 221 від 2012 року цифровий та кваліфікований електронний підпис залишаються єдиними електронними підписами, здатними відповідати вимогам пп. 1-12 ст. 1350 ЦК Італії.

З точки зору доказової цінності, стаття 21 КЦУ пропонує два варіанти.

Доказову силу електронного документа, підписаного електронним підписом, можна вільно оцінити з огляду на його об'єктивні характеристики якості, безпеки, цілісності та незмінності (ст. 21 § 1 КЦУ). Слід зазначити, що така сама доказова сила міститься у статті 20 § 1-bis КЦУ для електронного документа без підпису. Проте, видається правильним припустити, що наявність електронного підпису є достатньою для забезпечення документа більш високого ступеню достовірності, а отже, для обмеження розсуду суду. Комбіновані положення статті 21 § 2 КЦУ і статті 2702 ЦК Італії діють, щоб уникнути надання повної доказової цінності підпису, який поставлений без використання пристрою, який підписувач може підтримувати під його виключним контролем. Це означає, що доказова сила електронного документа, підписаного іншим способом, ніж розширений електронний підпис, визначатиметься судом за допомогою презумпцій.

В іншому випадку, згідно зі статтею 21 § 2 КЦУ, електронний документ, підписаний удосконаленням, цифровим або кваліфікованим електронним підписом, користується юридичною презумпцією справжності доказу, якщо сторона, що підписує, не заявляє, що походження заяв є неправдивим (як передбачено статтею 2702 ЦК Італії). Доказове значення, яке італійський законодавець присвоїв у 1997 році цифровому підпису, як еквіваленту традиційного листа, підписаного на папері, тепер поширюється на вдосконалений електронний підпис.

Документи, підписані цифровими та кваліфікованими електронними підписами, як зазначено у статті 21 § 2 КЦУ, вважаються підписаними власником пристрою підпису, якщо він не доведе протилежне.

Використання пристрою електронного підпису чи цифрового вважається власником, якщо він не доведе протилежне.

Ця презумпція виправдовується об'єктивними та відповідними гарантіями, які стверджуються з точки зору безпеки та надійності таких підписів, через криптографічний механізм та кваліфікований сертифікат, які

унеможливлують підробку підпису, а також можуть висвітлити будь-які подальші маніпуляції чи внесення змін до документа [213].

Незважаючи на чітке посилання на ст. 2702 ЦК Італії, науковці запропонували два суперечливі тлумачення, а отже, і дві різні реконструкції справжності електронного документа [140, с.44].

Згідно з однією точкою зору, дані в цифровому форматі (електронні листи) набувають чинності лише в тому випадку, якщо підписувач прямо визнає підписання документу, або якщо підпис юридично вважається визнаним через його засвідчення нотаріусом, відсутність заперечення підпису або негативний результат перевірки під час судового розгляду [202, с.73].

Інші вчені вважають, що електронний документ, підписаний цифровим, кваліфікованим або вдосконаленим електронним підписом, негайно набуде чинності юридично визнаної письмової форми, навіть за відсутності прямого чи неявного визнання підпису [142]. Ця друга думка була офіційно прийнята італійським законодавцем у минулому через поправки, внесені Законодавчим декретом № 10/2002 до статті 10 Указу Президента від № 445/2000 [131], але пізніше від нього відмовилися з набуттям чинності КЦУ.

Можливість передбачити автентифікацію будь-якої форми електронного підпису була б неефективною, якби документ, підписаний цифровим, кваліфікованим або вдосконаленим електронним підписом, вже був забезпечений законом (ст. 2702 ЦК Італії) з такою ж ефективністю, що й автентифікація. Однак протилежність тісно пов'язана з іншою дискусією щодо застосування до електронного підпису правил, що регулюють відмову від підпису та перевірку підпису, як це передбачено статтями 214–220 Цивільного процесуального кодексу Італії.

Цінність доказу, передбаченого ст. 2702 ЦК Італії, обумовлена явним визнанням підпису стороною, проти якої подано письмовий лист, або якщо підпис «юридично розглядається» як визнаний, щоб уникнути його заперечення. Якщо автор чітко визнає підпис, це саме по собі дає можливість

суду надати документу цінність доказу. Походження тверджень, що містяться в документі, та справжність підпису не є спірними фактами. Звідси випливає, що перевірка не потрібна [232].

З іншого боку, підпис вважається юридично визнаним, якщо автор підпису прямо не відмовився від підпису під час першого слухання або не подав заяви на захист після того, як документи були подані іншою стороною (іменується «мовчазне визнання»).

Якщо підпис буде визнано або засвідчено, то це означає, що автор не матиме можливості відмовитися від нього в судовому порядку (ст. 214 ЦПК Італії). Автор може стверджувати, що підпис є підробкою (статті 221 - 227 ЦПК Італії), у разі «мовчазного визнання» або з метою встановлення неправдивої заяви нотаріуса чи іншої уповноваженої посадової особи [130].

Якщо підпис не визнано (прямо чи законно), або його було відмовлено, контрагент, який подав документ у справі й все ще має намір покладатися на цей доказ, вимагатиме судової перевірки (ст. 216 ЦПК Італії) для встановлення достовірності підпису. Позитивна оцінка, що випливає з рішення суду, має однаковий ефект як визнання, так і засвідчення автентичності підпису.

Крім того, відповідно до ч. 2 ст. 216 ЦПК Італії, судова перевірка походження підпису може бути витребувана стороною як окрема судова справа не з метою використання документа як доказу в попередньому судовому розгляді, а для отримання однозначного рішення щодо автентичності документа. Норми, передбачені ст. 214 та наступними ЦПК Італії, як описано вище, застосовуються як до рукописного, так і до розширеного електронного підпису.

Ця заява не змінюється через імовірне використання пристрою власником, як зазначено у статті 21 § 2 КЦУ. Цю презумпцію, яка стосується лише цифрових та кваліфікованих електронних підписів, не можна ототожнювати до розпізнавання чи аутентифікації підпису: хоча останнє приписує цінність доказу використанню підпису, презумпція передбачає

перенесення тягара доказування. Справді, власник підпису (і власник пристрою) може подолати презумпцію, яка доводить протилежне.

Як зазначалося вище, італійські вчені запропонували кілька важливих аргументів для того, щоб не застосовувати положення, які забороняють автору ставити підпис до цифрових, кваліфікованих та вдосконалених електронних підписів. На думку деяких авторів [143], використання пристрою підпису (регулюється ст.ст. 32 і 35 ЦПК Італії) викликає розрив між волею підписувача та створенням зашифрованого коду. Процедура перевірки неможлива: вона здатна виявити лише використання пристрою підпису. Це не може продемонструвати, що власник використовував пристрій. Відповідно до цієї точки зору, у разі підробки підпису (використання пристрою неавторизованою третьою стороною), підписка буде віднесена до власника ключів, оскільки цифровий підпис (як і будь-який інший розширений підпис) є проста «печатка», прикріплена до документа наскрізь система шифрування [141]. Власник пристрою може вжити заходів щодо підробки лише для того, щоб довести несанкціоноване використання пристрою підпису третіми особами та подати докази походження документа.

Стаття 21 § 2 КЦУ передбачає, що «використання кваліфікованого електронного та цифрового підпису передбачається за рахунок власника, якщо він не доведе інше». Це пояснює, що презумпція обов'язково включає процес, за допомогою якого власник може (і повинен) довести, що він не використовував пристрій. Більше того, з огляду на відсутність італійської прецедентної практики щодо відмови від цифрового, кваліфікованого або розширеного електронного підпису, будь-яка інша думка виглядала б непослідовною або довільною.

Тягар доведення змінюється щодо права власності на цифровий або кваліфікований підпис. Оскільки використання пристрою підпису може (навіть зазвичай) виконувати хтось, хто не пов'язаний із пристроєм, недостатньо продемонструвати, що підпис був зроблений третьою стороною.

Необхідно буде надати докази того, що пристрій використовувався кимось іншим, ніж власник, і це відбулося поза контролем власника.

Власник, навіть якщо він втратив пристрій підпису, завжди зможе з'ясувати дату, час і місце, в якому пристрій було використано для підпису. Нормативно-правові положення передбачають безперервну діяльність із запису та транскрипції для користувачів і постачальників послуг підпису. Теоретично завжди можна довести, що пристрій підпису не використовувався кимось, хто в записаний час перебував в іншому місці.

У світлі вищевикладеного, зміщення тягара доказування здається найкращим способом збалансувати доказову діяльність. Сторона, яка відмовляється від електронного документа, має явні труднощі з доказом його автентичності, а відсутність контролю за пристроєм підпису найлегше може бути продемонстрована стороною, якій він належить. Цей аналіз здається узгодженим із думкою Верховного суду Італії, який стверджує, що тягар доказування має розподілятися відповідно до наближеності або наявності інструменту доказування, уникаючи неможливого або надмірно важкого тягара доказування в судовому процесі. Так само виконання ст. 2702 ЦК Італії та ст.ст. 214 – 220 ЦПК Італії щодо електронних підписів має на меті забезпечити еквівалентність електронного та рукописного документа, а також уникнути легкої відмови від електронного підпису його автором, а не призначити власнику підписного пристрою ті записи, які не належать до його волі та контролю. Крім того, відсутність судової практики та судових рішень щодо відхилення електронних підписів, здається, підкреслює їх цінність, оскільки вони вважаються засобами, які забезпечують високий рівень безпеки та цілісності, і їх важче оскаржити в суді, ніж власноручний підпис.

ВИСНОВКИ

Одержані в ході дисертаційного дослідження наукові результати дають підстави для висловлення таких висновків та пропозицій:.

1. Електронні докази – це дані (включаючи вихідні дані аналогових пристроїв або дані в електронній формі), які обробляються, зберігаються або передаються будь-яким виготовленим пристроєм, комп'ютером чи комп'ютерною системою або передаються через систему зв'язку, які можуть скласти фактичну інформацію про будь-який факт. Електронним доказом може бути будь-який електронний файл із цифрового або аналогового джерела. Це включає електронні листи, текстові повідомлення, миттєві повідомлення, файли та документи з жорстких дисків, електронні фінансові операції, аудіофайли та відеофайли тощо.

Електронний доказ - це вид засобу доказування, що містить дані про обставини справи, оригінал якого генерується, обробляється, зберігається або передається лише за допомогою електронного пристрою. Електронні докази за способом вираження інформації поділяються на два види: 1) інформація представлена в цифровій формі; 2) інформація, інтерпретована за допомогою програмного забезпечення у текст, звук, зображення тощо. Вказані способи вираження доказової інформації відрізняються за порядком використання їх в судовому процесі. Якщо інформація першого виду може бути досліджена лише експертом та залучається в судовий процес опосередковано через висновок експерта, то другий вид інформації може бути досліджений судом безпосередньо. На цій підставі побудовано дворівневу модель системи електронних доказів, залежно від особливостей джерел їх отримання та способу використання в процесі судового доказування: перший рівень - електронні докази, які за характеристиками матеріального носія та електронної інформації можуть бути безпосередньо доставлені в судові засідання та досліджені судом без використання спеціальних знань; другий рівень - електронні докази, які або через

особливості носія не можуть бути доставлені до суду, або специфіка електронної інформації, яку вони містять, не дозволяє їх дослідження без застосування спеціальних знань.

Цифровий доказ - це вид електронного доказу, який формується або перетворюється в числовий формат і може бути досліджений лише за допомогою ЕОМ.

2. Розширено перелік ознак електронних доказів та виділено з-поміж інших наступні ознаки: а) значний обсяг доказової інформації може бути отримано з одного джерела; б) простота передачі та копіювання відомостей з одного електронного носія інформації на інший; в) можливість віддаленого доступу до змісту електронного носія та інформаційно-телекомунікаційних систем (зокрема, до мережі «Інтернет»).

3. Усі файли в електронному форматі, включаючи повідомлення електронною поштою, електронні таблиці, вебсайти та документи для обробки текстів, містять метадані в тій чи іншій формі. Електронний файл повинен мати метадані, які допоможуть інтерпретувати призначення файлу. Такі дані можуть включати та автоматично братися з вихідного прикладного програмного забезпечення або надаватися особою, яка спочатку створила запис. Для суду можуть мати значення, зокрема, такі метадані: коли та як було створено документ (передбачуваний час і дата), тип файлу, ім'я передбачуваного автора (хоча це не обов'язково буде достовірним), розташування, з якого файл було відкрито, або де він зберігався, коли файл відкривався востаннє (передбачуваний час і дата), коли він востаннє змінювався, коли файл востаннє зберігався, коли він востаннє друкувався, ідентифікатор передбачуваних попередніх авторів, розташування файлу кожного разу, коли він зберігався, відомості про те, хто ще може отримати доступ до нього, і, у випадку електронної пошти, адреси прихованої копії. Доцільним вбачається запозичення наявної в судах країн загального права практики в разі подання до суду паперової копії електронного документа здійснювати роздруківку та подавати до суду не лише основний текст

документа, а й метадані, що сприятиме більш повному відображенню паперовою копією фактичних даних із оригіналу електронного документа та зручності сприйняття їх судом

4. Термін «електронний доказ» («electronic evidence») у нормативно-правових актах США не використовується, однак доволі докладно описаний на доктринальному рівні. «Електронні докази» визначаються американськими правознавцями як відомості, що обробляються, зберігаються або передаються будь-яким штучним пристроєм, комп'ютером або комп'ютерною системою, та які представляють ту чи іншу обставину, що має значення для справи, як більш-менш ймовірну.

Заслуговують на увагу положення пункту "d" правила 1001 Федеральних правил про докази, що встановлюють критерії розмежування оригіналу документа від його копії та містять положення, спрямовані безпосередньо на регулювання діяльності з використання комп'ютерної інформації у судовому процесі. Так, стосовно письмових матеріалів, записів і фотографій під оригіналом розуміється сам цей матеріал, запис або фотографія або їх аналог, що має те саме значення для особи, яка його виробила або випустила, що й оригінал. У той же час, для інформації, що зберігається в електронній формі, розмежування копії та оригіналу побудовано на іншій підставі - у цьому випадку оригіналом визнається будь-який аналог документа, візуально доступний для читання, роздрукований на принтері або іншому вивідному пристрої, за умови, що останній здатен адекватно відобразити інформацію.

У США відсутнє чітке розмежування доказів на види, а доказове право згруповано за типовими для практики проблемними ситуаціями. Як стверджують самі американські правознавці, статутне доказове право США, по суті, є закріпленням найважливіших та знакових судових рішень, узагальненою практикою, і носить, переважно, заборонний характер, тобто вказує, в яких випадках доказ не може бути визнаним допустимим. За таких обставин питання про те, чи є «електронні докази» самостійним видом

доказів, немає істотного значення для американських юристів.

У США електронні докази поділяються на види за типом (формою електронних даних). До них належать: письмове повідомлення (наприклад, документи, створені на комп'ютері), повідомлення, написані та надіслані електронною поштою, а також тексти, надіслані мобільним телефоном, сюди також включається запис голосу. Їх можна записати та зберегти на мобільному телефоні або в додатку. А ось цифрові фотографії є втіленням візуальних даних, роздрукованих або збережених у цифровому вигляді.

5. У цивільному процесуальному праві Англії та Уельсу також не виділяється такого окремого виду доказів як електронні докази, у Правилах цивільного судочинства йдеться лише про процедури та правила подання електронних документів. «Електронний документ» означає будь-який документ, що зберігається в електронній формі: електронна пошта та інші електронні засоби зв'язку, такі як текстові повідомлення і голосова пошта, текстові документи і бази даних, а також документи, що зберігаються на портативних пристроях, таких як карти пам'яті й мобільні телефони. На додаток до документів, які легко доступні з комп'ютерних систем та інших електронних пристроїв і носіїв, включаються документи, які зберігаються на серверах і системах резервного копіювання, і документи, які були видалені. Він також включає метадані та інші вбудовані дані, які зазвичай не видно на екрані або на роздруківці. В англійському праві термін «документ», крім письмових актів, охоплює також: а) карти, плани, графіки чи креслення; б) фотографії; в) диски, стрічки, звукові доріжки, інші пристрої, за допомогою яких звуки зафіксовані і можуть бути відтворені; г) фільми, негативи, що закріпили зорові образи та здатні їх відтворювати. Розрізняються поняття «електронне зображення» паперового документа та «власне електронний документ» - електронний документ, що зберігається у вихідній формі, в якій він був створений за допомогою комп'ютерної програми. Копіями документів називаються також копії магнітофонних записів, репродукції зображень і т.д.

6. Розвиток електронних доказів у Франції тісно пов'язаний з

електронним підписом та електронними листами, оскільки швидка поява нових комунікаційних засобів та інтенсивне використання інтернету викликали необхідність адаптації законодавства Франції до сучасних потреб.

Протягом тривалого часу письмові докази були синонімом паперових доказів, пізніше законодавець вирішив розв'язати цю проблему. Тому було вирішено, що необхідно встановити визначення письмових доказів, яке включатиме як традиційні, так і електронні письмові документи.

При цьому французькими юристами часто використовуються положення рекомендацій Ради Європи, згідно яких «електронні докази» означають будь-які докази, які виникають на основі даних, що містяться або створюються пристроєм, чия робота залежить від програмного забезпечення, або даних, що зберігаються чи передаються в системі, пристрої чи комп'ютерній мережі.

7. У німецькій процесуальній літературі під електронним документом прийнято розуміти текстові, аудіо-, відео- та програмні документи. Така думка ґрунтується на віднесенні електронного документа до речових доказів, і, відповідно, розумінні його як файлу, який може бути записаний на носії інформації. У цивільному процесі Німеччини загальні вимоги, що пред'являються до речових доказів, прийнято застосовувати й до електронних документів.

8. Італія була однією з перших країн у світі, яка прирівняла юридичну силу електронного документа, підписаного за допомогою цифрового підпису, до документів, написаних і підписаних на паперових носіях.

Визначення електронного документа в Італії, викладене наступним чином: «комп'ютерний документ: інформаційне відображення дій, фактів або юридично релевантних даних». Можливо, це визначення недостатньо детальне, проте з деякими корективами воно посилається на традиційне визначення документа. Також невід'ємною складовою електронного документа за законодавством Італії є електронний підпис, який надає такому документу юридичної сили. Електронний підпис - це набір даних в

електронній формі, доданих або логічно пов'язаних з іншими електронними даними, що використовуються як спосіб ідентифікації.

9. Існує велика кількість спільних ознак у законодавстві України та іноземних держав щодо електронних документів як доказів, який наділяє їх юридичною силою, наприклад, наявність електронного підпису є однією з спільних ознак. Під електронним підписом розуміють електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис.

Також у багатьох країнах наявний нормативно-правовий акт, що регулює порядок обміну цифровою інформацією між державними адміністраціями; зберігання електронних документів; створення національної мережі електронних документів та підписів. В Італії, наприклад, це Кодекс цифрового адміністрування, введений у законодавство декретом 82/2005, а в Україні - Закон України «Про електронні довірчі послуги».

Крім того, в Україні, як і в інших державах, законодавець розрізняє оригінал та копію електронного доказу, регламентує порядок їх зберігання та повернення. Однак з урахуванням можливості безперешкодного копіювання електронних доказів без обмеження кількості копій та без будь-якої втрати їх якісних характеристик у процесі копіювання можна прогнозувати виникнення певних практичних проблем у сторін спору щодо відокремлення оригіналу електронного доказу від його копії, а також щодо засвідчення копій електронних доказів.

На відміну від будь-якого іншого доказу, електронний доказ може зберігатися незмінним стільки, наскільки це може бути потрібним. Тоді як «традиційні» докази з часом втрачають свій зовнішній вигляд, якісні ознаки, а тому й доказову силу. Крім того, однією з основних ознак електронного документу як засобу доказування є відсутність зв'язку із конкретно визначеним матеріальним носієм, оскільки технічні засоби дозволяють копіювати такий документ необмежену кількість разів, користуватися ним у будь-який час, що не притаманно іншим засобам доказування.

10. Розбіжність у правовій регламентації правил щодо електронних доказів між Україною та іншими державами полягає у видовій належності електронних доказів. Так, наприклад, до речових доказів відносить електронні документи Цивільний процесуальний кодекс Німеччини, а у Франції та Італії електронні документи розглядають як письмові докази. Верховна рада України під час розробки та ухвалення нової редакції ЦПК прийняла концепцію, згідно якої електронні докази розглядаються як окремий вид засобу доказування. Вказане свідчить про автентичність вітчизняного юридичного механізму використання електронної інформації в процесі судового доказування, який характеризується поєднанням поліваріантності джерел отримання та фіксування електронних доказів із використанням традиційних процедур їх дослідження та оцінки.

Ще однією відмінністю є те, що норми ЦПК України дозволяють проведення огляду електронних доказів за їх місцезнаходженням у разі неможливості їх доставлення. Для правозастосування в США, наприклад, використовуються науковці та технічні фахівці для надання достовірних даних і фактів, які були представлені для доведення або спростування фактів, що мають значення для справи. У Франції ж доказова цінність електронної пошти може бути відновлена за допомогою судового виконавця та за допомогою комп'ютерного експерта, який зазначав би наявність електронних листів на сервері особи, яка заперечує їх існування або автентичність.

11. Запропоновано внести зміни до ЦПК України з метою оптимізації змісту ч. 1 ст. 100 та викласти її в наступній редакції: «Електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бірюков Р.М. Глобалізація та її вплив на правову сферу. Українсько-грецький міжнародний науковий юридичний журнал «Порівняльно-правові дослідження». 2009. № 2. С. 36-40.
2. Буркхард Шафер, Стівен Мейсон. Характеристики електронних доказів», у Стівена Мейсона та Деніела Сенга (ред.), Електронні докази. 4-е видання, Лондонський університет, 2017 р. С. 18-35
3. Вдовічена Л.І. Актуальність порівняльно-правової методології у науці фінансового права. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 156-160.
4. Гарі Едмонда, Крісті Мартіре та Мехари Сан Роке. Необгрунтоване право: проблеми з («експертними») доказами порівняння голосу. *Огляд права Melbourne University Law Review*. 2011. 52 с.
5. Герхард Люке. Право на інформацію в цивільному праві, *JuS*. 1986, 2 (3). Р.15-34.
6. Гладкий С.О. Методологія та організація наукових досліджень : навчально-методичний посібник. Полтава: ВНЗ Укоопспілки «ПУЕТ», 2016. 240 с.
7. Голубєва Н.Ю. Електронне судочинство: міжнародний досвід : монографія. Одеса: Фенікс, 2020. 204 с. URL: <http://dspace.onua.edu.ua/handle/11300/14039> DOI: 10.32837/11300.14039
8. Голубєва Н.Ю. Електронні докази в цивільному процесі Англії та Уельсу. *Новели цивільного процесуального законодавства: докази та доказування* : матеріали Міжнародної науково-практичної конференції (м. Одеса, 14 вересня 2020 р.). Одеса: Фенікс, 2020. 185 с. URL: <https://hdl.handle.net/11300/13083>
9. Грегорі П Джозеф, Сучасні візуальні докази (LJ Seminars Press

2009).

10. Грезіна О.М. Порівняльно-правовий метод дослідження проблем захисту прав учасників освітнього процесу. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України)* : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 21 трав. 2021 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2021. Т. 1. С. 105-107.

11. Декрет № 2001-272 від 30 березня 2001 р., прийнятий для застосування статті 1316-4 Цивільного кодексу щодо електронного підпису. ОВ від 31 березня 2001 р., 5070 с. URL: http://www.legifrance.gouv.fr/html/frame_lois_reglt.htm.

12. Деміан Шофілд. Використання зображень, створених комп'ютером, у судовому розгляді. *Digital Evidence and Electronic Signature Law Review* (2016). №13. URL: <https://doi.org/10.14296/deeslr.v13i0.2293>

13. Дж. Алекс Халдерман. Щоб не пам'ятати: атаки холодного завантаження на ключі шифрування. *Матеріали 17-ї конференції з безпеки симпозиуму Асоціації USENIX 2008*. 2009. URL: <https://citp.princeton.edu/research/memory/>

14. Дж. Кленсін. Простий протокол пересилання пошти. 2008. RFC 5321. URL: <https://tools.ietf.org/html/rfc5321>

15. Джон Д. Грегорі. Правила автентифікації та електронні записи. 2002. Can Bar Rev. P. 529-533

16. Джордж Л. Пол і Джейсон Р. Барон. Інформаційна інфляція: чи може правова система адаптуватися? 2007. RICH. J.L. & TECH 10. URL: <https://scholarship.richmond.edu/jolt/vol13/iss3/3/>

17. Джордж Р.С. Вейр і Стівен Мейсон. Джерела електронних доказів. *Електронні докази* : 4-е видання. Лондонський університет, 2017 р. С. 1-17.

18. Доповідь Комісії з цивільно-процесуального права. Федеральне

міністерство юстиції. стор.15. URL:
https://www.mlaw.gov.sg/files/Annex_C_Civil_Justice_Commission_Report.pdf/

19. Дорожня карта щодо цифровізації правосуддя в ЄС. Ares 2020. 4029305. URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12547-Digitalisation-of-justice-in-the-EU_en

20. Дрогозюк К.Б. Впровадження електронних доказів у цивільне судочинство Франції.. *Новели цивільного процесуального законодавства: докази та доказування* : матеріали Міжнародної науково-практичної конференції (м. Одеса, 14 вересня 2020 р.). Одеса : Фенікс, 2020. 185 с. URL: <https://hdl.handle.net/11300/13083>

21. Жаровська І.М. Щодо проблем методології теорії держави і права. *Вісник Національного університету Львівська політехніка. Серія: Юридичні науки*. 2015. №. 827. С. 138-141.

22. Закон про докази (процедури в інших юрисдикціях) 1975 р. (Evidence (Proceedings in other jurisdictions) Act 1975). URL: <https://www.legislation.gov.uk/ukpga/1975/34/contents>

23. Закон про докази в цивільному судочинстві 1968 р. (Civil Evidence Act 1968) URL: <https://www.legislation.gov.uk/ukpga/1968/64/contents>

24. Закон про докази у цивільному судочинстві 1972 р. (Civil Evidence Act 1972) URL: <https://www.legislation.gov.uk/ukpga/1972/30/contents/enacted>

25. Закон про докази у цивільному судочинстві 1995 р. (Civil Evidence Act 1995) URL: <https://www.legislation.gov.uk/ukpga/1995/38/contents>

26. Іванова А.Ю. Порівняльно-правовий метод як методологічний інструментарій прихильників наукового напрямку «політики права». *Альманах права*. 2012. Вип. 3. С. 175-178.

27. Інструкції з електронних доказів в цивільному і адміністративному судочинстві. 2019. URL: <https://rm.coe.int/lignes-directrices-sur-les-preuves-electroniques-et-expose-des-motifs/1680968ab6>

28. Кельман М. Методологія правознавства як світ організованих

форм мислення та діяльності дослідника. *Вісник Національного університету Львівська політехніка. Серія: Юридичні науки*. 2017. № 876. С. 61-67.

29. Клайв Фрідман. Огляд за допомогою технологій, схвалений для використання в судових процесах у Високому суді Англії. 2016. 13 с.

30. Козюбра М. Методологія правознавства і методологія права: співвідношення понять та їх особливості. *Право України*. 2014. № 1. С. 22-32.

31. Контролер мережевого інтерфейсу. URL: https://en.wikipedia.org/wiki/Network_interface_controller

32. Кравчук М. Сучасна методологія пізнання юриспруденції. *Підприємництво, господарство і право*. 2008. № 12. С. 114-117.

33. Кріс Бойд і Піт Форстер, Проблеми часу та дати в судово-обчислювальній техніці – приклад. *Digital Investigation*. 2004. №18. С. 45-51.

34. Локальна мережа. URL: https://en.wikipedia.org/wiki/Local_area_network

35. Мережеве сховище. URL: https://en.wikipedia.org/wiki/Network-attached_storage

36. Міранда Моубрей. Туман над Грімпен Майр: хмарні обчислення та закон. *Журнал із права, технологій та суспільства*. 2009. С. 131-136. URL: www.law.ed.ac.uk/ahrc/script-ed/vol6-1/mowbray.asp

37. Московчук Д. О. Обмеження щодо подання електронних доказів у законодавстві США. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)* : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса: Видавничий дім «Гельветика», 2022. Т. 2. С. 801-803.

38. Московчук Д.О. Загальна характеристика електронних доказів США та Німеччини. Реформування цивільного процесуального права в умовах інтеграційних процесів в Україні : матеріали Всеукраїнської науково-

практичної інтернет-конференції ім. Ю.С. Червоного. (м. Одеса, 18 грудня. 2020 р.) Одеса, 2020. С. 37-39.

39. Московчук Д.О. Кіліміченко А.О. Загальна характеристика допустимості та достовірності електронних доказів у законодавстві Малайзії та Республіки Сінгапур. *Часопис цивілістики*. 2021. № 41. С. 66-70.

40. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Індія. *Юридичний науковий електронний журнал*. 2022. №7/22. С. 559-562

41. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Узбекистан. *Право та державне управління*. 2022. №2. С. 304-308.

42. Московчук Д.О. Питання щодо особливостей електронних доказів у цивільному процесі Республіки Узбекистан. *Цивільне судочинство та виконавче провадження в умовах воєнного стану* : матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного (Одеса, 16 грудня 2022 р.) [Електронне видання] / за заг. ред. Н. Ю. Голубевої. Одеса : Фенікс, 2022. С. 47-49.

43. Московчук Д.О. Порівняльний аналіз законодавства України та країн англо-саксонської правової системи щодо подання доказів у цивільному процесі. *Підприємництво, господарство і право*. 2019. №4 (278). С. 55-60

44. Московчук Д.О., Даниляк Р.П. Загальна характеристика електронних доказів у законодавстві Сінгапуру. *Сучасна цивілістика: 15 років наукових звершень* : матеріали XV Міжнародної науково-практичної конференції. (м. Одеса, 22 трав. 2020 р.) Одеса, 2020. С. 364-365

45. Ніл Є. Система цивільного процесу Англії. Кембріджський ун-т. 2012. 554 с.

46. Оборотов Ю.М. Філософія права і методологія юриспруденції. *Проблеми філософії права*. 2003. Том 1. С. 41-43.

47. Оперативна пам'ять. URL: <https://en.wikipedia.org/wiki/Random->

access_Memory

48. Оптичне розпізнавання символів. URL:
https://en.wikipedia.org/wiki/Optical_character_recognitions

49. Павліченко Є.В., Голинська М.І. Становлення порівняльного правознавства та порівняльно-правової методології. *Правовий часопис Донбасу*. 2019. № 1 (66). С. 18-24.

50. Панов М. Проблеми методології формування категоріально-понятійного апарату юридичної науки. *Право України*. 2014. № 1. С. 50-60.

51. Пітер Соммер. Завантаження, журнали та захоплення: докази з кіберпростору. *Reprint of article in Journal of Financial Crime: 5JFC2*. pp 138-152. URL:
<http://www.pmsommer.com/dload01.pdf>

52. Подорожна Т.С. Аналіз способів застосування порівняльного методу в дослідженні явищ конституційно-правової дійсності. *Науковий вісник Львівського державного університету внутрішніх справ*. 2013. № 1. С. 84-88.

53. Подорожна Т.С. Місце і роль порівняльно-правового методу в методології конституційного процесу. *Часопис Київського університету права*. 2012. №. 3. С. 108-112.

54. Порівняльне правознавство: курс лекцій / Л.В. Голяк, А.С. Мацко, О.В. Тюріна. Київ. МАУП, 2004. 200 с.

55. Порівняльне правознавство : підручник / С. П. Погребняк, Д. В. Лук'янов, І. О. Биля-Сабадаш та ін. ; за заг. ред. О. В. Петришина. Харків. Право, 2012. С. 272 с.

56. Про адаптацію права доказів до інформаційних технологій, що стосуються електронного підпису : Закон 2000-230 від 13 березня 2000 р., ОВ від 14 березня 2000 р., с. 3968

57. Про систему електронних підписів, що застосовується в межах Співтовариства : директива 1999/93/ЄС Європейського Парламенту та Ради від 13 грудня 1999 р., JOCE від 19 січня 2000 р., L 13, с. 12. URL:
https://zakon.rada.gov.ua/laws/show/994_240#Text

58. Рабінович П. Методологія вітчизняного загальнотеоретичного праводержавознавства: деякі сучасні тенденції. *Право України*. 2014. № 1. С. 11-21.

59. Розмарі Паттенден. Аутентифікація «речей» в англійському праві: принципи надання матеріальних доказів у судах присяжних за загальним правом. *International Journal of Evidence and Proof*. 2008. 12 E & P 290. URL:

https://www.researchgate.net/publication/228178372_Authenticating_'Things'_in_English_Law_Principles_for_Adducing_Tangible_Evidence_in_Common_Law_Jury_Trials

60. Стівен Мейсон. Електронні докази та значення «оригіналу». 2009. 79 Amicus Curiae 26. URL: <https://sas-space.sas.ac.uk/2565/>

61. Тихомиров О.Д. Порівняльно-правові дослідження: проблеми ви значення компаративної природи, наукознавчого осмислення та систематизації : наукова доповідь. Київ-Львів: ЗУКЦ, 2012. Серія науково-методичних видань «Академія порівняльного правознавства». Випуск 29. 52 с.

62. Чванкін С.А. Інформаційні технології у доказуванні в цивільному процесі: теоретичні та практичні аспекти : дис. ... док. юрид. наук : 12.00.03. Одеса, 2021. 451 с.

63. Шигаль Д.А. Основні елементи теорії історико-правового порівняльного методу. *Правова доктрина – основа формування правової системи держави* : матеріали Міжнар. наук.-практ. конф., присвяч. 20-річчю НАПрН України та обговоренню п'ятитом. моногр. «Правова доктрина України», (Харків, 20–21 листоп. 2013 р.). Харків, 2013. С. 179–183.

64. Ю. Бруссолє, Основні положення постанови від 9 квітня 2019 р. щодо електронного підпису рішень господарських судів, ЗПУ від 20 вересня 2019 р. № 147. с. 12

65. Юркевич Х. Порівняльно-правовий метод в конституційно-правових дослідженнях. *Підприємництво, господарство і право*. 2019. Вип.

2. C. 156–160.

66. Abdel-Muttalib MAM. Search and criminal investigation in the digital computer and Internet crimes. *National Library*. 2006. P. 45-64. URL: http://scholar.google.com/scholar_lookup?&title=Search%20and%20criminal%20investigation%20in%20the%20digital%20computer%20and%20Internet%20crimes&publication_year=2006&author=Abdel-Muttalib%2CMAM

67. Abdul-Muttalib MAH, Qasim ZM, Aziz AA. A proposed model for the rules for adopting the digital evidence for evidence in computer crimes. 2003. Arab J 5:2253–2238

68. Abel. Urkundsbeweis durch digitale Dokumente. MMR 1998. S.644.

69. AG Erfahrt. MMR 2002. S.127. URL: <https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fmmr%2F2002%2Fcont%2Fmmr.2002.127.1.htm&pos=19>

70. Alessandro Mastomatteo and Benedetto Santacroce. Validità della firma elettronica: la firma biometrica come modello operativo avanzato. in *Corriere tributario*. 2012. pp 183 – 187

71. Allgeier. Ober die Beweiskraft im Recht unter besonderer Berücksichtigung von Kybernetik, Statistik und Wahrscheinlichkeit. MDR 1986. S.626.

72. Among many essays on this topic, Renato Borruso and Gianluigi Ciacci, *Diritto civile e informatica*, (Napoli: Edizioni Scientifiche Italiane – ESI, 2004), chapter 7, pp 410 – 423

73. Andrea Graziosi. Documento informatico (diritto processuale civile). *Enciclopedia del diritto*. Annali, II, 2, (Milano: Giuffrè, 2008), p 500

74. Arkfeld, M. R. *Electronic Discovery and Evidence*, Law Partner Publishing, 2005. LLC, Phoenix, AZ. P.1305 URL: <https://store.lexisnexis.com/products/arkfeld-on-electronic-discovery-and-evidence-skuusSku65900>

75. Art. 1367 C. civ. combiné avec l’art. 1 du décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique. URL:

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035676246/>

76. Article premier de la loi n° 1.383 sur l'Economie Numérique. URL: <https://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/9301A603E6FB1F33C12584FD002CC731!OpenDocument#:~:text=Le%20consommateur%20b%C3%A9n%C3%A9ficie%20aupr%C3%A8s%20du,sont%20pr%C3%A9cis%C3%A9s%20par%20ordonnance%20souveraine.>

77. Aurelio Gentili. Documento elettronico: validità ed efficacia probatoria. I contratti informatici, edited by Renato Clarizia, (Milano: UTET, 2007), pp 119-152.

78. Baker F. Requirements for IP Version 4 routers. 1995. *RFC*. 1812. URL: <https://tools.ietf.org/html/rfc1812>

79. Baumbach/Lauterbach/Albers/Hartmann. Kommentar zur ZPO. 65 Auflage. Munchen 2007. § 284. Rn.2

80. Becker. Elektronische Dokumente als Beweismittel im Zivilprozess. Frankfurt am Man 2004. S.9.

81. Bergfelder. Der Beweis im elektronischen Rechtsverkehr. Hamburg 2006. S.101

82. Biasiotti MA, Cannataci JA, Bonnici JPM, Turchi F (2018) Introduction: opportunities and challenges for electronic evidence. In: Handling and exchanging electronic evidence across Europe. Springer, Cham, Switzerland, pp 3–12.

83. BIOS. URL: <https://en.wikipedia.org/wiki/BIOS>

84. Bluetooth. URL: <https://en.wikipedia.org/wiki/Bluetooth>

85. Boente/Riehm. JURA 2001. S.796.

86. Borges. Verträge im elektronischen Rechtsverkehr. Munchen 2003. S.457.

87. Britz. Urkundebeweisrecht und Elektroniktechnologie. Munchen 1996. S.129;

88. Bundestagsdrucksache 14/4987. S.25. URL: https://dejure.org/Drucksachen/Bundestag/BT-Drs._14/4987

89. Bundestagsdrucksache 15/1508. S.56. URL:
<https://dserver.bundestag.de/btd/15/015/1501508.pdf>
90. Bundestagsdrucksache. 14/1191 (IuKD-Bericht). S.26. URL:
https://www.landtag-niedersachsen.de/drucksachen/drucksachen_14_2500/1001-1500/14-1191.pdf
91. Bundestagsdrucksache. 14/4662. S.44. URL:
<https://dserver.bundestag.de/btd/14/046/1404662.pdf>
92. C Kalt. Internet Relay Chat: Client Protocol. (2000) RFC 2812. URL:
<https://tools.ietf.org/html/rfc2812>
93. Casey E. Digital evidence and computer crime: forensic science, computers and the Internet. Academic Press, Cambridge, USA. 2011. P. 837. URL:
<https://rishikeshpansare.files.wordpress.com/2016/02/digital-evidence-and-computer-crime-third-edition.pdf>
94. Cass, 1civ., n. 09-68.555, 30 septembre 2010. URL:
<https://ru.scribd.com/document/149181180/SignatureElectroniqueendroitdesAffaires-Doc-1-27#>
95. Cass. Com., 4 octobre 2005, n. 04-15.195. URL:
<https://www.legifrance.gouv.fr/juri/id/JURITEXT000007050521>
96. Chang R.M. Why the plain view doctrine should not apply to digital evidence. *Journal of Trial and Appellate Advocacy*. Vol. XII. 2010. P. 51
97. Christine O Spiesel, Richard K Sherwin and Neal Feigenson, «Law in the age of images: the challenges of visual literacy», in A Wagner, T Summerfield and FSB Vanegas (eds), *Contemporary Issues of the Semiotics of Law* (Hart, 2005). P. 581. URL:
https://www.researchgate.net/publication/290860125_Law_in_the_age_of_images_The_challenges_of_visual_literacy_In_Wagner_A_Summerfield_T_Benavides_F_editors_Contemporary_issues_of_the_semiotics_of_law
98. Christopher Meyler. What evidence is left after disk cleaners? *Digital Investigation*. 2004. p. 183.
99. Civil Procedure Rules. URL:

<https://www.justice.gov.uk/courts/procedure-rules/civil>.

100. Code civil URL:
https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070721?etatTexte

101. Code de procédure civile URL:
https://www.legifrance.gouv.fr/codes/section_lc/

102. Craig Earnshaw and Sandeep Jadav. E-mail Tracing. *Computers & Law 7 for an introduction*. 2004. P. 56-78. URL: <https://www.scl.org/articles/690-e-mail-tracing>

103. Czeguhn. Beweiswert und Beweiskraft digitaler Dokumente im Zivilprozess. *JuS 2004*. S.124.

104. Decreto del Presidente della Repubblica 10 novembre 1997, n. 513, Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti costruenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 (Gazz. Uff. n. 60 del 13 marzo 1998). URL: <http://www.interlex.it/testi/dpr51397.htm>

105. Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (alla Gazz. Uff. n. 42 del 20 febbraio 2001, Suppl. ordinario n. 30). URL:
<https://www.parlamento.it/parlam/leggi/deleghe/00443dla.htm>

106. Decreto Legislativo 23 gennaio 2002, n. 10 Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche (Gazz. Uff. n. 39 del 15 febbraio 2002). URL:
<https://www.parlamento.it/parlam/leggi/deleghe/dlattcee.htm>

107. Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale (Gazz. Uff. n.112 del 16 maggio, Suppl. ordinario n. 93). URL:
https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/dl-7-marzo-2005-82_0.pdf

108. Decreto legislativo n. 235 del 30 dicembre 2010, Modifiche ed

integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009.
URL: <https://www.gazzettaufficiale.it/eli/id/2011/01/10/011G0002/sg>

109. Deveral Capps. Fitting a quart into a pint pot: the legal curriculum and matching the requirements of practice. 2013. P.10

110. Digicel (St Lucia) Ltd v Cable & Wireless Plc [2008] EWHC 2522 (Ch). URL: [https://uk.practicallaw.thomsonreuters.com/D-000-3548?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/D-000-3548?transitionType=Default&contextData=(sc.Default)&firstPage=true)

111. Digital Evidence and Electronic Signature Law Review. 2004. 1. pp 19-24.

112. Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques. URL: <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:31999L0093>

113. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p 12

114. Diritto Civile, edited by Silvio Martuccelli and Valerio Pescatore, (Milano: Giuffrè, 2011). 2011. pp 783-797.

115. Diritto dell'informazione e dell'informatica. 2012. P. 840.

116. Electronic evidence / General editor S. Mason. Croydon, 2012. 974 p.

117. Electronic serial number. URL: https://en.wikipedia.org/wiki/Electronic_serial_number

118. Electronic Signatures in Law. URL: <https://sas-space.sas.ac.uk/6518/1/ElectronicSignaturesStephenMason.pdf>

119. Englisch. Elektronisch gestutzte Beweisfuhrung im Zivilprozess. *Bielefeld*. 1999. S.32.

120. Eoghan Casey, Digital Evidence and Computer Crime. 3rd edn, Academic Press 2011. P.7.

121. EPROM. URL: <https://en.wikipedia.org/wiki/EPROM>.

122. Eric Caprioli. Vérification d'écriture en matière d'écrit électronique.

Communication Commerce Electronique n°10, Octobre 2006, comm.149

123. Ernst. Beweisprobleme bei E-Mail und anderen Online-Willenserklärungen. *MDR*. 2003. S.1090-1096.

124. Federal Rules of Civil Procedure. URL: <https://www.law.cornell.edu/rules/frcp>

125. Federal Rules of Evidence. Washington, 2013. 142 p.

126. Feral-Schul. La jurisprudence de la cour de cassation en matière de preuve électronique. URL: www.feral-avocats.com

127. For a commentary of the Digital administration code, see Giovanni Duni, ‘Amministrazione digitale’, *Enciclopedia del diritto. Annali*, I [Accertamento – Tutela], (Milano: Giuffrè, 2007), pp 13-47.

128. For an analysis of this particular issue, and the fact that judges in jurisdictions across the globe have also accepted this proposition, see *Electronic Signatures in Law*, pp 221-253.

129. For the meaning of ‘document’ in a digital context, see Stephen Mason, general editor, *Electronic Evidence*, chapter 10. P 426. URL: <https://library.oapen.org/bitstream/handle/20.500.12657/39391/9781911507079.pdf>

130. Francesca Ferrari. Il codice dell’amministrazione digitale e le norme dedicate al documento informatico. *Rivista di diritto processuale civile*. 2007. pp 415-431.

131. Francesco Ricci, *Scritture private e firme elettroniche*, (Roma: Luiss University Press, 2003), pp 163-176.

132. Franssen V., Berrendorf A., Corhay M. La collecte transfrontière de preuves numériques en matière pénale. Enjeux et perspectives européennes. *e-Revue internationale de droit pénal*. 2019. P. 24-31.

133. G. Camarillo (ed.). *Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability*. 2009. RFC 5694. URL: <https://tools.ietf.org/html/rfc5694>

134. Garante per la protezione dei dati personali. General Guidelines on

biometric identification and graphometric signature. Linee guida in materia di riconoscimento biometrico e firma grafometrica. issued on 21 May 2014. URL: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3132361>

135. Gautrais V. Preuve des reproductions : vues d'ailleurs! *CDST*. 2014 [en ligne], n. 4

136. Geis. Die neue Signaturverordnung: Das Sicherheitssystem für die elektronische Kommunikation. *K&R*. 2002. S.61

137. General guidelines for electronic bundles in The Supreme Court of the United Kingdom and Judicial Committee of the Privy Council URL: <https://www.supremecourt.uk/procedures/electronic-bundle-guidelines.html>

138. Geoff Fellows. Peer-to-peer networking issues - an overview. *Digital Investigation*. 2004. #3. P. 67-81

139. Géraldine Vial, Olivier Leclerc et Étienne Vergès. Preuves scientifiques et technologiques CA Paris, 15 mai 2019, n. 18/26775

140. Giovanni Verde. Prove nuove. *Rivista di diritto processuale*. 2006. pp 35-52.

141. Giusella Finocchiaro. Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale. *Contratto e impresa*. 2011. pp 495-504.

142. Giusella Finocchiaro. Il valore probatorio del documento informatico e firma digitale. in *Contratto e impresa*. 2002. pp 76-85.

143. Giusella Finocchiaro. Tecniche di imputazione della volontà negoziale; le firme elettroniche e la firma digitale. I contratti informatici, edited by Renato Clarizia, (Milano: UTET, 2007). pp 201-233.

144. Golubtsov VG Electronic evidence in the context of e-justice. *Civil Procedure Bull*. 2019. 9(1). Pp. 170-188. <https://doi.org/10.24031/2226-0781-2019-9-1-170-188>

145. Gorelick, Jamie S., Marzen, Stephen Esq., Solum, Lawrence B., *Destruction of Evidence* Aspen Law and Business, Aspen, Co, 1989. URL:

<https://lawcat.berkeley.edu/record/1151009>

146. Gravesen/Dumortier/Van Eecke. Die europäische Signaturrechtlinie - Regulative Funktion und Bedeutung der Rechtswirkung // MMR 1999. S.581.

147. Greger y: Zöller. § 138 para. 8a. URL:
<https://www.cambridge.org/core/journals/german-law-journal/article/preparing-germany-for-the-21st-century-the-reform-of-the-code-of-civil-procedure/653046EA1A39A6F0A16D813BB2683366>

148. Gregory P Joseph, Modern Visual Evidence (Law Journal Press 2009)
 4. P. 37 URL:
https://books.google.com.ua/books?id=T8bapbdhCAQC&printsec=copyright&redir_esc=y#v=onepage&q&f=false

149. Haverinen H. and Salowey J. (eds.), 'Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)' (2006) RFC 4186
 <<https://www.ietf.org/rfc/rfc4186.txt>

150. Heidi H. Harralson. Forensic document examination of electronically captured signatures. *Digital Evidence and Electronic Signature Law Review*. 2012. 9. pp 67-73.

151. Hierry Aballéa. Signature électronique, quelle force pour la présomption légale? D.2004, p. 2235.

152. Huber. Modernisierung der Justiz? ZRP. 2003. S.268 URL:
<https://www.jstor.org/stable/23428490>

153. Ibrahim KM. The electronic evidence in cybercrime from the website. National Library. 2020. P. 156-187

154. In re Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. p. 598

155. International Mobile Station Equipment Identity. URL:
https://en.wikipedia.org/wiki/International_Mobile_Station_Equipment_Identity

156. International mobile subscriber identity. URL:

[https://en.wikipedia.org/wiki/ International_mobile_subscriber_identity](https://en.wikipedia.org/wiki/International_mobile_subscriber_identity)

157. JCI Communication, fascicule 4740 courrier électronique, v. note n. 143.
158. Jean-Michel Bruguière, « *La difficile preuve par e-mail* », Rev. Lamy dr. civ. 2011 p. 179-199
159. Justizkommunikationsgesetz v.22.3.2005. BGB11. 837. URL: <https://www.degruyter.com/document/doi/10.1515/9783110898705.83/pdf>
160. Kahsay Debesu, Andualem Eshetu Law of Evidence. 2009. P. 210. URL: [https://uogqueensmcf.com/wp-content/uploads/2020/BA%20Modules/LAW%20\(LL.B\)/3rd%20year/3rd%20year%20-seme-2/Law%20of%20Evidence.pdf](https://uogqueensmcf.com/wp-content/uploads/2020/BA%20Modules/LAW%20(LL.B)/3rd%20year/3rd%20year%20-seme-2/Law%20of%20Evidence.pdf)
161. Kessler G.C. Judge' Awareness, Understanding, and Application of Digital Evidence. Miami, 2010. P. 26
162. Klensin J. and Padlipsky M. Unicode format for Network Interchange. 2008. RFC 5198. URL: <https://tools.ietf.org/html/rfc5198>
163. Komnios. Die elektronische Signatur im deutschen und griechischen Recht. Frankfurt am Main 2007. S.182
164. La consécration légale de la preuve électronique, Janvier-Février 2014. URL: <https://www.caprioli-avocats.com/fr/informations/le-juge-et-la-preuve-electronique-reflexions-sur-le-projet-de-21-197-0.html#:~:text=L'%C3%A9crit%20%C3%A9lectronique%20sign%C3%A9%20%C3%A0,que%20son%20int%C3%A9grité%20soit%20garantie.>
165. La firma elettronica, si apre un nuovo capitolo', Studium juris, 2002, pp 1431-1434
166. La metafora e il diritto nella normativa sulla cosiddetta «firma grafometrica». Diritto dell'informazione e dell'informatica, 2013, pp 1 – 16, p
167. Lamber J. Electronic Disclosure in England & Wales. *Digital Evidence and Electronic Signature Law Review*. 2006. Vol. 3. P. 73-76.
168. Lampe. Falschung technischer Aufzeichnungen. *NJW*. 1970. S. 1097
169. Legge 17 dicembre 2012, n. 221 Conversione in legge, con

modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese (Gazz. Uff. n.294 del 18 dicembre 2012, Suppl. Ordinario n. 208). URL: <https://www.gazzettaufficiale.it/eli/gu/2012/12/18/294/so/208/sg/pdf>

170. Legge 25 marzo 1997, n.59 Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa (Gazz. Uff. n. 63 del 17 marzo, Suppl. ordinario n. 56/L). URL: <http://www.comune.jesi.an.it/MV/leggi/l59-97.htm>

171. Legge 29 luglio 2003, n. 229, Interventi in materia di qualità della regolazione, riassetto normativo e codificazione – Legge di semplificazione 2001 (Gazz. Uff. n. 196 del 25 agosto 2003). URL: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2003;229>

172. LG Bonn. CR 2002. S.293. URL: <https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Bonn&Datum=07.08.2001&Aktenzeichen=2%20O%20450/00>

173. Luc Grynbaum. Le droit de l'écrit électronique : un frein au commerce en ligne. RLDI 2011. P.67

174. Luc Grynbaum. Preuve par écrit électronique non sécurisé d'une inscription de créance. Communication Commerce Electronique n.3, mars 2006, note n. 48.

175. M Crispin. Internet Message Access Protocol - Version 4rev1. 2003. RFC 3501. URL: <https://tools.ietf.org/html/rfc3501>

176. M. Day, DCC Digital Curation Manual Installment on Metadata (UKOLN 2005) URL: www.dcc.ac.uk/resources/curation-reference-manual/completed-chapters/metadata

177. Mason S., Seng D. Electronic evidence. University of London Press. 2017. URL: <https://doi.org/10.14296/517.9781911507079>

178. Matteo Giacomo Jori. L'efficacia probatoria dell'e-mail. *Giurisprudenza italiana*. 2005, pp 1028-1030.

179. Münchener Kommentar zur Zivilprozessordnung (Band 1 bis 3). München 2008. Vor § 415. Rn.5.
180. Mobile identification number. URL: https://en.wikipedia.org/wiki/Mobile_identification_number
181. Mobility management. URL: https://en.wikipedia.org/wiki/Mobility_management#TMSI
182. Münchener Kommentar zur Zivilprozessordnung (Band 1 bis 3). München 2013. § 371. Rn.8. URL: <https://beckassets.blob.core.windows.net/product/toc/11109643/musielak-kommentar-zivilprozessordnung-zpo-9783800645312.pdf>
183. Myers J. and Rose M. Post Office Protocol - version 3. 1996. RFC 1939. URL: <https://tools.ietf.org/html/rfc1939>
184. Naim S. Research and investigation mechanisms for information crime in Algerian law. Master Thesis. 2013. P. 144
185. Natalino Irti. Forma del contratto e prova. in *Le prove nel diritto civile e tributario*, edited by Cesare Glendi, Salvatore Patti and, Eugenio Picozza. Torino: Giappichelli, 1986. p. 33
186. OLG Köln. CR 2003. S.55. URL: <https://dejure.org/dienste/vernetzung/rechtsprechung?Text=OLGR%202003,%208>
187. Palmer G. A Road Map for Digital Forensic Research. *the First Digital Forensic Research Workshop (DFRWS)*. November, Utica, New York. 2001. URL: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf
188. Paolo Tonalini. La sottoscrizione elettronica dei documenti, in *Studium juris*, 1997. p 442
189. Paul Torremans, Holyoak and Torremans Intellectual Property Law. 8th edn, Oxford University Press 2016. P. 612
190. Per Overbeck. The burden of proof in the matter of alleged illegal

downloading of music in Denmark. 2010. 7 Digital Evidence and Electronic Signature Law Review 87

191. PRACTICE DIRECTION 31B – DISCLOSURE OF ELECTRONIC DOCUMENTS. URL: https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31/pd_part31b

192. PRACTICE DIRECTION 51U - DISCLOSURE PILOT FOR THE BUSINESS AND PROPERTY COURTS URL: <https://www.justice.gov.uk/courts/procedure-rules/civil/rules/practice-direction-51u-disclosure-pilot-for-the-business-and-property-courts>

193. Rapp. Rechtliche Rahmenbedingungen und Formqualitat elektronischer Signaturen. Mtinchen 2002. S.39.

194. Redeker. EU-Signaturrechtlinie und Umsetzungsbedarf im deutschen Recht. CR. 2000. S.455.

195. Rivista trimestrale di diritto processuale civile. 2003. pp 53 – 80.

196. RoBnagel. Digitale Signaturen im europaischen elektronischen Rechtsverkehr. K&R. 2000. S.317.

197. RoBnagel. Recht der Multimedia-Dienste. Mtinchen 2004. Rn.14.

198. RoBnagel/Fischer-Dieskau. Elektronische Dokumente als Beweismittel. NJW. 2005. S.807.

199. Rosenberg/Schwab/Gottwald. Zivilprozessrecht. Munchen, 2004. URL: <https://beckassets.blob.core.windows.net/product/toc/20019020/rosenberg-zivilprozessrecht-9783406710858.pdf>

200. Rothstein P.F. Evidence: State and Federal Rules. St. Paul, 1991. P. 1.

201. Salvatore Patti. Documento. Digesto delle discipline privatistiche, sezione civile. VII. (Torino: Utet, 1994), pp 1-13.

202. Salvatore Patti. L'efficacia probatoria del documento informatico. *Rivista di diritto processuale*. 2000. pp 60-92.

203. Sanuel H Solomon, Joanna Gallant and John P Esser (eds), The Science of Courtroom Litigation: Jury Research and Analytical Principals. ALM Publishing 2009. P 368

204. Scheindlin, Shira A., Wangkeo, Kanchana. *Electronic Discovery. Sanctions in the TwentyFirst Century*. 11 Mich. Telecomm. Tech. Rev. 71-124, 2004. URL: <https://repository.law.umich.edu/mttlr/vol11/iss1/3/>
205. Schneider. *Beweis und Beweiswiirdigung*. 5.Auflage. Miinchen 1994. § 2. S.16
206. See Marina Pietrangelo, *La società dell'informazione tra realtà e norma*, (Milano: Giuffrè, 2007), pp 43-63.
207. *Signaturgesetz vom 16. Mai 2001 (BGB1. I S. 876)*. URL: https://elektronische-steuerpruefung.de/literatur/uni_stach.pdf
208. Sosnitza/Gey. *Zum Beweiswert von E-Mails, technische Hintergrunde und rechtliche Konsequenzen*. *K&R*. 2004. S.467.
209. Staudinger-Bearbeiter. *Kommentar zum BGB*. B.Auflage. Berlin 2007. S. 341.
210. Stephen Mason (ed). *International Electronic Evidence (British Institute of International and Comparative Law*. URL: <https://library.oapen.org/bitstream/handle/20.500.12657/39391/9781911507079.pdf>
211. Stephen Mason. *Electronic banking and how courts approach the evidence*. *Computer Law and Security Review*. April 2013. Volume 29, Issue 2. pp 144-151.
212. Stephen W Teppler. *Digital data as hearsay*. *Digital Evidence and Electronic Signature Law Review*. 2009. 6, 7, 9 n 18
213. Studi e materiali. *Quaderni trimestrali del Consiglio Nazionale del Notariato: La sicurezza giuridica nella società dell'informazione*, Suppl. n. 1, 2008, pp 127-139.
214. Svein Yngvar Willassen. *Forensics and the GSM mobile telephone system*. 2003. *Intl J of Digital Evidence*. #2. URL: <https://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf>
215. *The characteristics of electronic evidence in digital format' in Stephen*

Mason, general editor. *Electronic Evidence*. 3rd edn, LexisNexis Butterworths, 2012. P. 23-70

216. The Digital Tower of Babel. *Digital Evidence and Electronic Signature Law Review*, 5 (2008), pp 183 – 186.

217. The Guardian : newspaper (Лондон, 2 серпня 2016 р.) URL: www.theguardian.com/technology/2016/aug/02/apple-replaces-gun-emoji-water-pistol-revolver-violence-debate

218. The Sedona Conference Cooperation Proclamation. July 2008. URL: <http://www.ned.uscourts.gov/internetDocs/cle/2011-01/TSC%20Cooperation%20Proclamation.pdf>

219. The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. *European Committee on Legal Co-operation (CDCJ)*. Strasbourg, 27 July 2016. A comparative study and analysis. URL: <https://rm.coe.int/168070029>

220. Thomas M Dunlap and Nicholas A Kurtz. Electronic evidence in torrent copyright cases. *Digital Evidence and Electronic Signature Law Review*. 2011. 8. p. 171

221. Thomas/Putzo. Kommentar zur ZPO. § 371. Rn.4. URL: <https://jurcase-shop.com/thomas-putzo-zpo-kaufen-der-standard-kommentar-zur-zpo/>

222. Tribunal de Première instance, 09 juin 2005, SBM SAM c/ N. <https://www.legifrance.gouv.fr/juri/id/JURITEXT000006946366>

223. Tribunal de Première instance, 11 avril 2013, X c/ Y. URL: <https://www.tribunaux-rechtbanken.be/fr/tribunaux/tribunal-de-premiere-instance>

224. Tribunal du travail, 16 mars 20000, S. c/ SAM GTS Monaco Access.

225. Viefhues. Das Gesetz iiber die Verwendung elektronischer Kommunikationsformen in der Justiz. *NJW*. 2005. S.1009. URL: <https://dip.bundestag.de/vorgang/.../96089>

226. Vinton Cerf. RFC 20 - 'ASCII format for Network Interchange. 1969. *RFC 20*. URL: <https://tools.ietf.org/html/rfc20>

227. Warken C. Classification of electronic data for criminal law purposes. *Eucrim: the European Criminal Law Associations' forum*. 2018. vol 4. Freiburg, Germany. p. 3.
228. Waxse J y Williams v Sprint/United Management Company 230 FRD 640, 646-47 (D.Kan. 2005). URL: <https://dockets.justia.com/docket/kansas/ksdce/2:2003cv02200/42746>
229. Website of the European Commission: <https://ec.europa.eu/digital-single-market/en/blockchain-technologies>
230. West African Gas Pipeline Co Ltd v Willbros Global Holdings Inc [2012] EWHC 396 (TCC). URL: <http://www.bailii.org/ew/cases/EWHC/TCC/2012/396.html>
231. Wi-Fi. URL: <https://en.wikipedia.org/wiki/Wi-Fi>
232. Widely, Giovanni Buonomo and Aniello Merone. La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio. *Diritto dell'informazione e dell'informatica*. 2013. pp 255-286.
233. Winett J. M. The EBCDIC codes and their mapping to ASCII. 1971. RFC 183. URL: <https://tools.ietf.org/html/rfc183>
234. Yergeau F. UTF-8, a transformation format of ISO 10646. 2003. RFC 3629. URL: <https://tools.ietf.org/html/rfc3629>
235. Zoller/Geimer. Kommentar zur ZPO. 26.Auflage. Koln 2007.
236. Zubulake v. UBS Warburg LLC, No. 02 Civ. 1243 (SAS), 2004 U.S. Dist. LEXIS 13574, at *35 (S.D.N.Y. July 20, 2004).

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації, в яких опубліковані основні наукові результати дисертації:

1. Московчук Д.О. Порівняльний аналіз законодавства України та країн англо-саксонської правової системи щодо подання доказів у цивільному процесі. *Підприємництво, господарство і право*. 2019. №4 (278). С. 55-60
2. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Індія. *Юридичний науковий електронний журнал*. 2022. №7/22. С. 559-562
3. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Узбекистан. *Право та державне управління*. 2022. №2. С. 304-308.
4. Московчук Д.О. Кіліміченко А.О. Загальна характеристика допустимості та достовірності електронних доказів у законодавстві Малайзії та Республіки Сінгапур. *Часопис цивілістики*. 2021. № 41. С. 66-70.

Публікації, які засвідчують апробацію матеріалів дисертації:

5. Московчук Д.О., Даниляк Р.П. Загальна характеристика електронних доказів у законодавстві Сінгапуру. *Сучасна цивілістика: 15 років наукових звершень* : матеріали XV Міжнародної науково-практичної конференції, (м. Одеса, 22 трав. 2020 р.) Одеса, 2020. С. 364-365
6. Московчук Д.О. Загальна характеристика електронних доказів США та Німеччини. *Реформування цивільного процесуального права в умовах інтеграційних процесів в Україні* : матеріали Всеукраїнської науково-

практичної інтернет-конференції ім. Ю.С. Червоного, (м. Одеса, 18 грудня. 2020 р.) Одеса, 2020. С. 37-39.

7. Московчук Д. О. Обмеження щодо подання електронних доказів у законодавстві США. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф., (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса: Видавничий дім «Гельветика», 2022. Т. 2. С. 801-803.*

8. Московчук Д.О. Питання щодо особливостей електронних доказів у цивільному процесі Республіки Узбекистан. *Цивільне судочинство та виконавче провадження в умовах воєнного стану : матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного, (Одеса, 16 грудня 2022 р.) [Електронне видання] / за заг. ред. Н. Ю. Голубєвої. Одеса : Фенікс, 2022. С. 47-49.*

ВІДОМОСТІ ПРО АПРОБАЦІЮ МАТЕРІАЛІВ ДИСЕРТАЦІЇ

Дисертація підготовлена на кафедрі цивільного процесу Національного університету «Одеська юридична академія». Результати дисертаційного дослідження обговорювалися на засіданнях кафедри цивільного процесу Національного університету «Одеська юридична академія». Основні положення дисертації оприлюднені на 4 міжнародних та всеукраїнських науково-практичних конференціях, круглих столах: XV Міжнародній науково-практичній конференції «Сучасна цивілістика: 15 років наукових звершень» (м. Одеса, 22 травня 2020 р.); Всеукраїнській науково-практичній інтернет-конференції ім. Ю.С. Червоного «Реформування цивільного процесуального права в умовах інтеграційних процесів в Україні» (м. Одеса, 18 грудня 2020 р.); Міжнародній науково-практичній конференції «Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)» (м. Одеса, 17 червня 2022 р.); Всеукраїнській науково-практичній конференції ім. Ю.С. Червоного «Цивільне судочинство та виконавче провадження в умовах воєнного стану» (Одеса, 16 грудня 2022 р.).

«ЗАТВЕРДЖУЮ»

Ректор

Національного університету

«Одеська юридична академія»

професор Віктор ЗАГОРОДНИЙ



АКТ

**про впровадження наукових розробок дисертаційного дослідження
Московчука Д.О. на тему: «Електронні докази у країнах
континентального та загального права: порівняльно-правове
дослідження» на здобуття наукового ступеня вищої освіти доктора
філософії з галузі знань 08 «Право» за спеціальністю 081 «Право»
в освітній процес Національного університету
«Одеська юридична академія»**

Комісія у складі: голови – проректора Галини УЛЬНОВОЇ, членів комісії – завідувачої кафедри цивільного процесу, професора Неллі ГОЛУБСОВОЇ, декана факультету цивільної та господарської юстиції, доцента Дениса КОЛОДІНА, начальника навчально-методичного відділу Людмили КУЗНЕЦОВОЇ, директора центру організації освітньої підготовки та інформаційно-аналітичної роботи Анатолія ПАВЗЮКА, склали цей акт про те, що наукові статті та тези конференцій за результатами дисертації аспіранта кафедри цивільного процесу Національного університету «Одеська юридична академія» Дмитра Московчука на тему: «Електронні докази у країнах континентального та загального права: порівняльно-правове дослідження» поданої на здобуття наукового ступеня вищої освіти доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право», впроваджені в освітній процес Національного університету «Одеська юридична академія» у рамках викладання занять всіх видів зі студентами з дисциплін: «Цивільний процес», «Європейський цивільний

процес», «Доказування та докази в цивільному судочинстві», «Розгляд окремих категорій справ у судах», «Практика ЄСПЛ у цивільному судочинстві», а також у науково-дослідній роботі студентів університету.

Рекомендовано до використання у навчальному процесі наступні публікації Д.О. Московчука:

1. Московчук Д.О. Порівняльний аналіз законодавства України та країн англо-саксонської правової системи щодо подання доказів у цивільному процесі. *Підприємство, господарство і право*. 2019. №4 (278) С. 55-60
2. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Індія. *Юридичний науковий електронний журнал*. 2022. №7/22. с. 559-562
3. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Узбекистан. *Право та державне управління*. 2022. №2. с. 304-308.
4. Московчук Д.О. Кіліміченко А.О. Загальна характеристика допустимості та достовірності електронних доказів у законодавстві Малайзії та Республіки Сінгапур. *Часопис цивілістики*. 2021. № 41. с. 66-70
5. Московчук Д.О., Даниляк Р.П. Загальна характеристика електронних доказів у законодавстві Сінгапуру. *Матеріали XV Міжнародної науково-практичної конференції «Сучасна цивілістика: 15 років наукових звершень»* (м. Одеса, 22 трав. 2020 р.) Одеса. 2020. с. 364-365
6. Московчук Д.О. Загальна характеристика електронних доказів США та Німеччини. *Матеріали Всеукраїнської науково-практичної інтернет-конференції ім. Ю.С. Червоного «Реформування цивільного процесуального права в умовах інтеграційних процесів в Україні»* (м. Одеса, 18 грудня. 2020 р.) Одеса. 2020. с. 37-39
7. Московчук Д.О. Загальна характеристика окремих засобів альтернативного вирішення спору у Великобританії. Альтернативні

- способи вирішення цивільних спорів : матеріали круглого столу (Одеса, 29 березня 2021 р.) [Електронне видання] / за заг. ред. д.ю.н., професора Н. Ю. Голубєвої. НУ «Одеська юридична академія». Одеса. Фенікс. 2021. с.37-41
8. Московчук Д. О. Обмеження щодо подання електронних доказів у законодавстві США. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів ХХІ століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса: Видавничий дім «Гельветика», 2022. Т. 2. С. 801-803.

Голова комісії

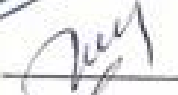


проф. Галина УЛЬЯНОВА

Члени комісії



доц. Денис КОЛОДІН



проф. Неллі ГОЛУБЄВА



Анатолій ПАВЗІЮК



Людмила КУЗНЕЦОВА

Південне міжрегіональне управління
Міністерства юстиції (м. Одеса)

Заступник начальника Південного
міжрегіонального управління Міністерства
юстиції Південного міжрегіонального
управління Міністерства юстиції (м.
Одеса)



Дмитрій БУРЯЧЕНКО

2022 року

АКТ

**про впровадження наукових розробок дисертаційного дослідження
МОСКОВЧУКА Дмитра на тему: «Електронні докази у країнах
континентального та загального права: порівняльно-правове
дослідження» на здобуття наукового ступеня вищої освіти доктора
філософії з галузі знань 08 «Право» за спеціальністю 081 «Право»**

Комісія у складі: голови: заступника начальника Управління - начальника відділу судової роботи та міжнародного співробітництва в Одеській області Управління судової роботи та міжнародного співробітництва Південного міжрегіонального управління Міністерства юстиції (м. Одеса) Сергія КОРОТКОВА; членів: головного спеціаліста відділу судової роботи та міжнародного співробітництва в Одеській області Управління судової роботи та міжнародного співробітництва Південного міжрегіонального управління Міністерства юстиції (м. Одеса) Дмитра ПОДОРЯНА та головного спеціаліста відділу судової роботи та міжнародного співробітництва в Одеській області Управління судової роботи та міжнародного співробітництва Південного міжрегіонального управління Міністерства юстиції (м. Одеса) Анни СТАРОСТИНОЇ, склали цей акт з приводу того, що результати дисертаційного дослідження Московчука Дмитра на тему «Електронні докази у країнах континентального та загального права: порівняльно-правове дослідження» за спеціальністю 081 «Право» на здобуття наукового ступеня доктора філософії, впроваджено у процес підготовки працівників Південного міжрегіонального управління Міністерства юстиції (м. Одеса).

Комісія вважає, що викладені у публікаціях пропозиції та висновки заслуговують практичного використання у діяльності Південного міжрегіонального управління Міністерства юстиції (м. Одеса). Рекомендовано до використання наступні публікації:

1. Московчук Д.О. Порівняльний аналіз законодавства України та країн англо-саксонської правової системи щодо подання доказів у цивільному процесі. *Підприємство, господарство і право*. 2019. №4 (278) С. 55-60
2. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Індія. *Юридичний науковий електронний журнал*. 2022. №7/22. с. 559-562
3. Московчук Д.О. Особливості електронних доказів у цивільному процесі республіки Узбекистан. *Право та державне управління*. 2022. №2. с. 304-308.
4. Московчук Д.О. Кіліміченко А.О. Загальна характеристика допустимості та достовірності електронних доказів у законодавстві Малайзії та Республіки Сінгапур. *Часопис цивілістики*. 2021. № 41. с. 66-70
5. Московчук Д.О., Даниляк Р.П. Загальна характеристика електронних доказів у законодавстві Сінгапуру. *Матеріали XV Міжнародної науково-практичної конференції «Сучасна цивілістика: 15 років наукових звершень»* (м. Одеса, 22 трав. 2020 р.) Одеса. 2020. с. 364-365
6. Московчук Д.О. Загальна характеристика електронних доказів США та Німеччини. *Матеріали Всеукраїнської науково-практичної інтернет-конференції ім. Ю.С. Червоного «Реформування цивільного процесуального права в умовах інтеграційних процесів в Україні»* (м. Одеса, 18 грудня. 2020 р.) Одеса. 2020. с. 37-39
7. Московчук Д.О. Загальна характеристика окремих засобів альтернативного вирішення спору у Великобританії. Альтернативні способи вирішення цивільних спорів : матеріали круглого столу (Одеса, 29 березня 2021 р.) [Електронне видання] / за заг. ред. д.ю.н., професора Н. Ю. Голубсової. НУ «Одеська юридична академія». Одеса. Фенікс. 2021. с.37-41
8. Московчук Д. О. Обмеження щодо подання електронних доказів у законодавстві США. Європейський вибір України, розвиток науки та

національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса: Видавничий дім «Гельветика», 2022. Т. 2. С. 801-803.

Заступник начальника Управління –
начальник відділу судової роботи та
міжнародної правової допомоги в Одеській області
Управління судової роботи та міжнародної
правової допомоги Південного
міжрегіонального управління
Міністерства юстиції (м. Одеса)

Сергій КОПОТКОВ

Головний спеціаліст відділу судової роботи
та міжнародної правової допомоги в Одеській області
Управління судової роботи та міжнародної
правової допомоги Південного
міжрегіонального управління
Міністерства юстиції (м. Одеса)

Дмитро ПОДОРЯН

Головний спеціаліст відділу судової роботи
та міжнародної правової допомоги
Управління судової роботи та міжнародної
правової допомоги Південного
міжрегіонального управління
Міністерства юстиції (м. Одеса)

Катерина ЛУКАСЕВИЧ