УДК 347.941 : 004
DOI https://doi.org/10.32847/ln.2021.15.04

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

РОЗКРИТТЯ ЕЛЕКТРОННИХ ДОКАЗІВ ЗА ЗАКОНОДАВСТВОМ США

Постановка завдання. У нашому взаємопов'язаному світі цифрове середовище ставить величезні завдання перед практикуючими юристами (суддями й адвокатами) у будь-якій країні, але стаття присвячена виключно федеральному цивільному процесу в Сполучених Штатах (США). Оскільки країна є батьківщиною світових технологічних лідерів, таких як Microsoft, Apple, Google, Amazon чи Facebook, неминуче необхідно взяти до уваги те, як федеральна судова влада США справляється із цим питанням, якщо ми хочемо знайти якісь орієнтири серед цифрової турбулентності. У роботі не розглядаються кримінальні провадження, а фокус виключно на цивільних процесах, які стосуються судового вирішення позовів однієї особи чи групи проти іншої, та відповідної цивільної процедури, яка встановлює правила, за якими суд проводить ці процеси. Одержання цифрових доказів (чи електронно збереженої інформації – ESI – загальний термін, використовуваний Федеральними правилами цивільного судочинства США – FRCP) у хмарних системах складніше, ніж у попередніх комп'ютерних середовищах [9, с. 304, 308].

У 2006 році у FRCP були внесені поправки, які встановлюють ESI як окремий об'єкт розкриття, що призвело до появи так званого електронного розкриття – досудового й в основному приватного процесу між сторонами з метою запиту, отримання та надання ESI. Однак у той час хмарні обчислення не мали тієї актуальності, яку вони мають нині. Зі зростанням присутності й важливості хмарних обчислень юридичним операторам, таким як учасники справи, необхідно знайти спосіб витребувати й використовувати ESI в рамках цивільного процесу, а суддям – проводити відповідний процес електронного розкриття доказів. Цифрові докази виходять за рамки традиційних комп'ютерних систем, які генерували, обробляли й зберігали дані в одному місці й характеристики яких сприяли створенню «оригінального» електронного розкриття доказів.

У 1938 році FRCP набрав чинності, і процес розкриття доказів був офіційно включений до закону, дозволяючи сторонам «оглядати власність іншої сторони, а також вивчати й копіювати документи інших сторін». Таким чином, незважаючи на можливі недоліки моделі, учасникам судових процесів було забезпечено доступ до зростаючого обсягу бізнес-документування своїх контрагентів у рамках досудового процесу, який, на думку Верховного суду США, має приватний характер і не є частиною протоколу суду [11].

Система розкриття містила три основні гілки: документи, допити й показання. Система виявлення була розроблена для того, щоб «виявити сильні й слабкі сторони справи кожної сторони на ранній стадії, тим самим сприяючи якнайшвидшому врегулюванню» допомогою саморегулюючого процесу [7, с. 547, 557] – дві важливі характеристики, які залишаються суттєвими для електронного розкриття доказів.

У 2006 році до FRCP було внесено деякі поправки з метою адаптації правил щодо процесу виявлення до все актуальнішого цифрового середовища, що дозволило створити

концепцію електронного зберігання інформації (ESI) [17]. Такий оновлений підхід став початком того, що нині прийнято називати електронним розкриттям інформації.

Формулювання завдання дослідження. Мета роботи – розглянути розкриття електронних доказів за законодавством США.

Виклад основного матеріалу. Визначення електронного розкриття доказів. Такий особливий процес існує поряд із традиційними трьома напрямами розкриття інформації. Йоргенсен визначає електронне виявлення як «вилучення, виготовлення та оцінку відповідних даних із певних сховищ даних, метаданих і зберігачів» [8, с. 299]. У більш стислому вигляді стандарт ISO, що розробляється для електронного виявлення, описує його як «процес виявлення релевантних ESI або даних однією або обома сторонами, що беруть участь у розслідуванні, і будь-які випливаючі з нього дії» [5, с. 313, 327]. Широке охоплення ESI підтверджується FRCP, який дає підстави для цього специфічного процесу в таких термінах:

Сторони можуть отримати інформацію з будь-якого непривілейованого питання, що стосується позову або заперечення будь-якої сторони, включаючи існування, опис, характер, зберігання, стан і місцезнаходження будь-яких документів або інших матеріальних речей, а також особу й місцезнаходження осіб, яким відомо про будь-який предмет, що виявляється (Fed. R. Civ. P. 26 (b) (1)).

Два елементи такого юридичного визначення – привілейована інформація та критерії релевантності – заслуговують на коротке пояснення, оскільки вони містять мінімальні межі кожного процесу електронного виявлення.

Привілейована інформація знаходиться поза сферою електронного розкриття інформації. Загалом привілейована інформація стосується інформації, захищеної законом, і не підлягає розкриттю. У галузі права найпоширенішим привілеєм є зв'язки між адвокатом і клієнтом, проте залежно від законів штату й, звичайно, від конкретної справи можуть бути й інші види привілеїв: наприклад, справа про медичну недбалість може містити конфіденційні зв'язки між лікарем і пацієнтом. Оскільки як зміст повідомлень, так і метадані можуть містити привілейовану інформацію, запобігання розкриття таких даних вважається складною чи неможливою задачею, тобто ситуацією, коли неминуче щось, що є привілейованим чи захищеним, буде розкрито, ненавмисно чи інакше.

Критерій релевантності. Цей аспект спрямовано на встановлення меж електронного розкриття доказів. Сторони повинні обмежити процес необхідною інформацією, пов'язаною з претензіями й запереченнями проти позову; якщо сторони не дійшли згоди щодо того, яка інформація релевантна, обмеження мають бути встановлені постановою суду (FRCP 26 (b) (1)). Відповідно до своїх дискреційних повноважень суди можуть розширити «з поважної причини» обсяг розкриття, якщо воно вважається таким, що виходить за рамки предмета позову [15, с. 427, 433].

Інформація, що зберігається в електронному вигляді (ESI). У поправках до FRCP від 2006 року термін було прийнято для позначення інформації, що обробляється цифровим способом. Поняття було навмисно широким, щоб охопити всі типи комп'ютерних даних, які використовуються натепер, а також майбутні технологічні розробки. Отже, сюди підходить все: «записи, креслення, графіки, діаграми, фотографії, звукозаписи, зображення та інші дані або добірки даних, що зберігаються на будь-якому носії, з якого інформація може бути отримана або безпосередньо, або, за необхідності, після перекладу стороною, що відповідає іншій стороні, в розумну придатну для використання форму» (FRCP 34(a) (1) (A)). Таким чином, стає зрозумілим, що будь-який електронний пристрій, здатний виробляти, передавати або зберігати дані, генеруватиме ESI. Натепер таке обладнання, як персональний комп'ютер, а також мобільні пристрої, такі як ноутбуки або смартфони,

можна вважати звичайними джерелами ESI, але IoT (Інтернет речей) ще більше розширить сферу їх застосування. Корисно згадати найпоширеніший приклад: автомобілі. За словами Гудмана, «раніше автомобілі працювали на бензині. Нині вони працюють на коді <...> Автомобіль, що зійшов із конвеєра у 2015 році, має від сімдесяти до ста бортових комп'ютерів». Ці бортові комп'ютери дозволять дізнатися, наприклад, навички водія, що є досить корисною інформацією для страхових компаній [10, с. 246].

Автори схильні підкреслювати різні характеристики ESI, переважно на противагу паперовим документам. У такому сенсі для Герра й Макінсона основними характеристиками ESI є постійність (навіть після «видалення» дані можуть зберігатися в комп'ютерному пристрої), обсяг (обсяг даних, що постійно зростає) і мінливість (легко піддаються змінам) [2, с. 390, 406]. На думку Тепплера, цифрові дані «за своєю природою податливі або мінливі» [13, с. 213, 217]. Нема потреби викладати більше думок, оскільки більшість із них визнає, що на відміну від незмінного характеру паперового документа інформація, створена, оброблена й збережена бінарною мовою (нулі й одиниці, що становлять цифровий світ), може вважатися вразливою.

Метадані:

а) *Визначення*. У рамках ESI однією з найбільш значущих підкатегорій для юридичних цілей є метадані, які зазвичай згадуються як дані про дані, хоча такого широкого поняття недостатньо для повного охоплення цього типу інформації. У своєму глосарії версії 2014 Седонська конференція розглядає метадані як «загальний термін, що використовується для опису структурної інформації файлу, яка містить дані про файл, на відміну від опису вмісту файлу». Судовий експерт та адвокат Крейг Болл розуміє під цим терміном «докази, що зазвичай зберігаються в електронному вигляді, які описують характеристики, походження, використання, структуру, зміну й достовірність інших електронних доказів» [1]. Як приклад, федеральний окружний суд штату Мериленд визначив метадані як:

«(i) інформацію, вбудовану в нативний файл, що зазвичай не доступна для перегляду або друку з програми, яка створила, відредагувала або змінила такий нативний файл;

(ii) інформацію, яка автоматично генерується в результаті роботи комп'ютера або іншої інформаційно-технологічної системи під час створення, зміни, передачі, видалення або іншого маніпулювання «рідним файлом» користувачем такої системи» [14].

У цілому, можна стверджувати, що на відміну від будь-якого документа метадані містять інформацію, що генерується комп'ютерними системами й пов'язана з конкретним електронним файлом;

b) *Важливість*. До прийняття поправок до FRCP у 2006 році Седонська конференція зменшила значущість метаданих, залишивши їх провадження чи збереження залежно від угоди між сторонами чи ухвали суду, вважаючи, що в більшості випадків вони не матимуть істотної доказової сили [16]. Деякі суди дотримувалися такої позиції, вважаючи метадані непотрібними або такими, що не мають доказової сили, тим більше коли сторона, що запитує, не вказала на необхідність їх отримання.

Проте деякі суди відійшли від такого підходу й ще до поправок 2006 року почали примушувати сторони, що запитуються, до надання метаданих. Наприклад, у справі 2004 року про порушення авторських прав [4] метадані були визнані необхідними для визначення того, були деякі музичні файли отримані з компакт-диска або з одного джерела (p2p-клієнта); інша справа 2005 року [6] стосувалася незаконного присвоєння комерційної таємниці, і метадані були корисні позивачу, оскільки він хотів установити, чи в комп'ютері відповідача використовувався комп'ютерний код, що порушує авторські права; нарешті, суперечка, пов'язана з незаконним використанням вікового критерію для звільнення співробітників у ході скорочення

штату [19], стосувалася використання метаданих, що містяться в деяких електронних таблицях excel, і суд після заперечень відповідача вирішив, що метадані повинні бути надані в незмінному вигляді, якщо не буде досягнуто згоди або не буде подано належне обґрунтування.

У зв'язку з таким розвитком подій у 2007 році Седонська конференція внесла зміни до своїх керівних принципів, визнавши тепер необхідність створення метаданих, які дозволять стороні, що запитує, отримати доступ, провести пошук та оцінити інформацію в тому вигляді, в якому вона була створена.

Усього три роки знадобилося Седонській конференції, щоб прийняти метадані як важливий аспект електронного розкриття інформації. Початкова зневага до такого типу даних була швидко залишена, коли адвокатура й деякі суди усвідомили важливість такого аспекту в деяких випадках. Як підкреслює суддя, серед кількох причин, через які метадані можуть бути релевантними, є три основні:

(i) їхня допомога в перевірці справжності ESI;

(ii) своя позиція, щоб визначити, чи є документ привілейованим;

(iii) їх полегшуючий характер проведення пошуку інформації [18].

Крейг Болл, експерт та учасник судового процесу, також наводить деякі причини, щоб оцінити цінність метаданих, оскільки, за його словами, вони «проливають світло на походження, контекст, справжність, надійність і поширення електронних доказів, а також дають підказки про поведінку людини». Це електронний еквівалент дезоксирибонуклеїнової кислоти, балістичної експертизи й експертизи відбитків пальців, що має порівнянну здатність виправдовувати й викривати [1].

Розкриття та запит даних. Загальні положення FRCP дозволяють запитуючій стороні вимагати ESI широким чином, із зобов'язанням виконання вимог, установлених Правилом 34 (b) (1) та єдиним законним обмеженням у вигляді привілейованої інформації та вищезгаданих критеріїв релевантності. Оскільки в США відсутній загальний закон про захист даних (за винятком положень у галузі охорони здоров'я, фінансів та освіти), персональні дані (або персонально ідентифікована інформація) не мають такого ж рівня захисту, як в Європейському Союзі, тому оцінка їх надання в контексті електронного пошуку повинна проводитись у кожному конкретному випадку. Після подання скарги обидві сторони змушені готуватися до низки засідань, регульованих правилами 16 і 26 (f) FRCP. Як тільки спір стає реальністю, FRCP передбачає два основні шляхи щодо одержання ESI:

a) Розкриття інформації. Правило 26 встановлює загальне зобов'язання сторін надавати своїм контрагентам інформацію, не чекаючи запиту про розкриття, під опікою чи контролем FRCP (34 (a) (1) (A)). Оскільки релевантність є єдиним критерієм, що міститься у FRCP для оцінки того, є ESI релевантною чи ні, і закон не розглядає категоризацію ESI, розкриття є досить суб'єктивною стадією, адже лише деякі провадження звільняються від початкового розкриття. Таке розкриття відбувається в рамках засідань та являє собою перший підхід до наявних доказів, пов'язаних із позовом. Відповідач повинен надати позивачу основну інформацію у справі, щоб обидві сторони могли краще оцінити спір;

b) Запит даних. Після обміну розкриттями протилежна сторона може запросити додаткову інформацію щодо претензій або захисту будь-якої сторони, піднятої в змагальних документах, використовуючи процес запиту про виявлення інформації. У той час, як розкриття інформації належить до обов'язку відповідача надати загальну інформацію, про яку йдеться в правилі 26, запит на електронне виявлення міститься в правилі 34 й здійснюється в рамках конференції сторін. FRCP не встановлює конкретного часу для подання запитів, але встановлює час для відповіді на них: за загальним правилом, сторона, яка подає запит, «має відповісти письмово про-

тягом 30 днів після його вручення»; термін може бути продовжений за згодою сторін або за рішенням суду (34 (b) (2) (A).). Сторона, яка потребує більш конкретної інформації, ніж розкрита, може вимагати від свого контрагента надати відповідну ESI. Сторони можуть домовитися про конкретні обмеження або кількість запитів, оскільки FRCP не містить жодних юридичних обмежень. Такі Правила встановлюють широкі рамки щодо запиту, оскільки сторони можуть запитати «будь-які зазначені документи або ESI <...>, що зберігаються на будь-якому носії», у той час, як сторона може заявити заперечення, щоб протистояти провадженню. Цей другий шлях отримання даних залежить від здібностей чи досвіду адвоката, враховуючи, що загальне зобов'язання розкриття більше застосовується.

Збереження. Запитувана сторона (зазвичай, відповідач) зобов'язана «ідентифікувати, знаходити й зберігати інформацію та матеріальні докази, які мають стосунок до конкретного й ідентифікованого судового процесу». FRCP не конкретизує цей обов'язок, оскільки під час обговорення поправок 2006 року вважалося, що встановити загальне правило досить складно. Отже, прецедентне право стало основним джерелом практики електронного виявлення. У рамках такого обов'язку найважливішими стали два аспекти: коли виникає зобов'язання щодо збереження (тригер) та як це зобов'язання може бути виконане (юридичне утримання):

a) Тригер. У справі Silvestri v. General Motors суд ухвалив, що обов'язок щодо збереження «виникає не тільки під час судового процесу, але й поширюється на той період до початку судового процесу, коли сторона розумно повинна знати, що докази можуть мати стосунок до очікуваного судового процесу» [12]. Таке «розумне передбачення» буде стандартом визначення моменту, коли дані мають бути під рукою. Очевидно, що під час подачі скарги збереження ESI є явно неминучим обов'язком, тому ситуація не становить проблеми для визнання існування зобов'язання. Незрозумілим залишається момент, коли очікуваний судовий процес може спричинити виникнення зобов'язання. Якщо, наприклад, внутрішня електронна пошта натякне на можливість порушення патенту, чи може це повідомлення привести до виникнення зобов'язання? Досі, як стверджує суддя Нью-Йорка Пек, «ніхто <...> не зміг дати справедливого й певного приводу для збереження». Його порада: краще зберігати цінну пропозицію, враховуючи, що виникнення обов'язку може навіть вважатися подією за роки до подання позову «через просту поінформованість про суперечку інших представників галузі» [16];

b) Судове утримання. Воно визначається як повідомлення, видане в результаті поточного або обґрунтовано очікуваного судового розгляду, аудиту, юридичного чи нормативного питання, яке припиняє нормальне розпорядження або опрацювання ESI. Як до початку офіційного судового розгляду, так і після подання скарги сторона, що запитує, може надіслати повідомлення своєму контрагенту з проханням не видаляти інформацію та зберегти її. Наприклад, отримання повістки до суду або скарги, отримання повістки до суду або офіційне повідомлення про те, що організація є об'єктом урядового розслідування, повідомляє контрагенту про те, що він зобов'язаний зберегти відповідну інформацію. З боку відповідача достовірна інформація про те, що він є об'єктом судового позову, може бути достатньою для виникнення обов'язку щодо збереження. У такому сенсі будь-яке повідомлення, наприклад, електронний лист, може розглядатися як повідомлення.

Як тільки виникає привід для збереження інформації, сторона, що запитує, зобов'язана визначити, які дані повинні бути збережені та як це можна зробити. Залежно від конкретного випадку, звичайно, інформація може міститися в декількох файлах, а може потребувати ретельного й дорогого цифрового пошуку. Показовим прикладом наслідків такого утри-

мання є справа *Zubulake v UBS Warburg*, де стороні-виробнику та її адвокату наполегливо рекомендується визначити відповідну інформацію, щоб забезпечити її доступність.

Пропорційність. У контексті електронного розкриття інформації такий принцип належить до балансу між потребами запитувача для відповідної інформації та тягаря та витрат відповідача, пов'язаних із виробництвом ESI. Дійсно, сторона, що запитує, може запросити будь-який вид ESI, але це не зобов'язує контрагента зберігати або надавати все, що запитується. Для досягнення такого принципу у FRCP існують стримування та противаги. З одного боку, запит повинен мати стосунок до позову чи заперечення. З іншого боку, сторона не може забезпечити ESI, якщо доступ до неї не представляється можливим «через надмірне навантаження або вартість» (FRCP P. 26 (b) (2) (B)).

Хоча пропорційність прямо не прописана у FCRP, в юридичній практиці широко визнається існування принципу, і навіть деякі правила штатів, наприклад, наявні в штаті Юта, вже містять його (Utah R. Civ. P. 26 (b) (1) – (b) (3)). Пропоновані поправки до FCRP безпосередньо включити принцип пропорційності для заохочення суддів і сторін використовувати його активніше.

Знищення. Непостійність, властива ESI, є основою концепції. У справі *Zubulake* суддя Шейндлін визначив псування як «знищення або значну зміну доказів, або незбереження майна для використання іншою особою як доказу в поточному або розумно прогнозованому судовому процесі» (Zubulake v UBS Warburg 229 F.R.D. 422 (S.D.N.Y. 2004). У процесі електронного розкриття інформації завжди є ризик не отримати відповідні докази.

Умисна або випадкова втрата або знищення ESI може стати кошмаром як для позивача, так і для відповідача. Як правило, повідомлення про позов або судовий арешт тягне за собою зобов'язання зберегти всі дані, що стосуються спору, щоб уникнути їх розголошення, тому із цього моменту сторона-відповідач має бути максимально обережною.

Санкції. Ураховуючи ризик знищення, єдиним юридичним засобом стримування для запобігання такого ризику є накладення санкцій, які залежать тільки від розсуду судді першої інстанції та повинні оцінюватись у кожному конкретному випадку. Санкції регулюються правилом 37 FRCP і можуть бути застосовані сторонами як примус до розкриття інформації або виявлення. Хоча правило містить кілька прикладів (наприклад, відмова від позову або винесення рішення заочно), діапазон не винятковий. У справі *Пейс, LLC v. Hyundai Motor Co.* суд вважає найжорсткішими санкціями «відмову від позову або судового рішення заочно». Трохи нижче в спектрі знаходяться розпорядження про заборону, які визнаються суворими санкціями, хоча й не такими різкими, як попередні. Дозвіл несприятливих висновків або спростовна презумпція також вважається суворою санкцією. Іншими словами, погане поводження ESI може призвести до того, що запитувана сторона ризикує програти справу. Однак не всі санкції пов'язані з такими серйозними наслідками. Суди не схильні вирішувати спори за допомогою палиці, тому вони зазвичай намагаються запровадити мінімальні санкції, необхідні для забезпечення справедливого процесу. Варто зауважити, що грошові санкції співіснують із незвичайнішими, такими як директиви, які вимагають від порушника «повідомляти кожного позивача в майбутніх справах протягом 5 років про минулі порушення розкриття» або додаткові розкриття та відстрочки оплати [15, с. 442].

Такої короткої панорами достатньо, щоб підкреслити загальні труднощі, пов'язані з накладенням санкцій, спрямованих на проведення справедливого, швидкого й недорогого процесу електронного розкриття, як це передбачено FRCP. Якщо до такого й так складного сценарію додати хмарні обчислення, можна очікувати ще більших труднощів.

Чинна законодавча база, що регулює ESI, датується 2006 роком, понад п'ятнадцять років тому. На той момент локальні комп'ютерні системи були найпоширенішими, тому можна сказати, що більшість ESI могли обробляти внутрішні менеджери. Однак FRCP не виключає можливості для третьої сторони (наприклад, аутсорсингових компаній) бути змушеною надати документи й матеріальні речі або дозволити перевірку, якщо це необхідно, в рамках процесу електронного розкриття доказів. Визнаючи постійно зростаючий потік даних, суд вказав у 2008 році, що зобов'язання зберігати й створювати ESI не можна уникнути лише «за допомогою простого способу зберігання їх у третьої сторони». Коли відповідна ESI знаходиться у володінні третьої сторони, суди повинні оцінити, чи має сторона практичну можливість або законне право отримати ESI на вимогу, чи зберегла будь-яке право чи можливість керувати третьою стороною, яка володіє ESI (Flagg v. Detroit, 252 F.R.D. 346, 347 (E.D. Mich. 2008)). Такий аналіз буде особливо актуальним щодо постачальників хмарних послуг.

Аутентифікація ESI виходить за рамки електронного розкриття доказів. Після того, як ми в цілому прояснили функціонування процесу електронного виявлення, доречно виділити той факт, що такий процес не стосується аутентифікації виявленого ESI – це тема, яка заслуговує окремого дослідження. У США автентичність документів, які використовуються як докази в цивільних справах, не є особливою перешкодою для подолання, оскільки все ще є переважаючим підходом із використанням традиційної моделі пошуку додаткових непрямих доказів. Меншість експертів вважає, що до ESI потрібно ставитися інакше, в основному через притаманну їй ненадійність і низьку планку, яка наразі існує для неї в судах. Важливо вказати різницю, оскільки лише один відсоток справ досягає фази судового розгляду: ситуація, яка робить процес електронного відкриття набагато актуальнішим у судовій системі США, ніж проблема аутентифікації. Таку прагматичну визначну позицію підтвердила конференція Sedona Conference, яка процитувала суддю Грімма, щоб пояснити недостатню увагу, яку приділяє автентифікації: оскільки електронне відкриття є дорогим процесом, «не має сенсу витрачатися на всі турботи й витрати, щоб отримати електронну інформацію лише для виключення її з доказів або відхилити від розгляду під час спрощеного судового рішення, оскільки ініціатор не може закласти достатню основу для її визнання» [3].

Тому, хоча стаття зосереджується лише на проблемах створення та збереження ESI, характерних для процесу електронного розкриття доказів, а не на питаннях її аутентифікації, необхідно враховувати, що деякі труднощі, пов'язані з раннім керуванням ESI в рамках e-discovery, стосуються можливості використання певної інформації (особливо метаданих) для судових цілей. Перспектива використання ESI як доказу в судовому засіданні є суттю електронного розкриття доказів, але правила такого процесу відрізняються від тих, які застосовуються, коли суд повинен проаналізувати його прийнятність, а присяжні повинні оцінити релевантність і вплив доказів.

Висновки. Огляд процесу електронного розкриття доказів дозволяє виявити деякі особливості такої системи. Будучи досудовою стадією, процес спонукає обидві сторони до ранньої оцінки доказів щодо спору. Якщо припустити, що тільки 1% конфліктів зрештою не вирішується, то таку здебільшого саморегульовану систему можна вважати успішною.

Познайомившись з електронним розкриттям і характеристиками хмарних обчислень, ми зможемо краще оцінити характерні проблеми, які вони несуть із собою для електронного розкриття та, що важливіше, для цілей статті; те, як сторони й судді у вітчизняному цивільному процесі можуть впоратися з аналогічними проблемами.

Анотація

Стаття зосереджується на проблемах створення та збереження інформації в електронній формі, характерної для процесу електронного розкриття доказів. Процес електронного розкриття доказів, будучи досудовою стадією, спонукає обидві сторони до ранньої оцінки доказів щодо спору. Така система дозволяє зрештою вирішити абсолютну більшість справ без безпосереднього судового розгляду. І хоча система є здебільшого саморегульована, вона має певні правила, передбачені Федеральними правилами цивільного судочинства США. Водночас електронні докази виходять за рамки традиційних комп'ютерних систем, які генерували, обробляли й зберігали дані в одному місці й характеристики яких сприяли створенню «оригінального» електронного розкриття доказів. До FRCP було внесено деякі поправки з метою адаптації правил щодо процесу виявлення до все актуальнішого цифрового середовища, що дозволило створити концепцію електронного зберігання інформації. Такий оновлений підхід став початком того, що нині прийнято називати електронним розкриттям інформації. Процедура містить правила визначення переліку доказів, надання їх сторонам, збереження та санкцій за порушення таких правил. Ураховуючи підвищений ризик знищення електронних доказів, єдиним юридичним засобом стримування для запобігання ризику є накладення санкцій, які залежать тільки від розсуду судді першої інстанції та повинні оцінюватись у кожному конкретному випадку. Окрема увага звертається на метадані, які дозволяють встановити походження інформації, контекст, справжність, надійність і багато інших деталей, необхідних для правильної оцінки доказів. Потрібно враховувати, що деякі труднощі, пов'язані з електронними доказами в рамках e-discovery, стосуються можливість використання певної інформації (особливо метаданих) для судових цілей. Перспектива використання інформації в електронній формі як доказу в судовому засіданні є суттю електронного розкриття доказів, але правила такого процесу відрізняються від тих, які застосовуються, коли суд повинен проаналізувати їх прийнятність.

Ключові слова: електронні докази, розкриття доказів, цивільний процес США, цивільне судочинство США, цифрові докази, інформація в електронній формі.

Kalamaiko A.Yu. Disclosure of electronic evidence under U.S. law

Summary

The article focuses on the problems of creating and storing information in electronic form, typical of the process of electronic disclosure of evidence. The process of electronic disclosure of evidence, as a pre-trial stage, the process encourages both parties to an early assessment of the evidence in the dispute. This system ultimately allows the vast majority of cases to be resolved without direct trial. And although the system is largely self-regulating, it has certain rules provided by the Federal Rules of Civil Procedure of the United States. At the same time, electronic evidence goes beyond traditional computer systems, which generated, processed and stored data in one place, and whose characteristics contributed to the creation of "original" electronic evidence disclosure. The FRCP was amended to adapt the rules on the detection process to an increasingly relevant digital environment, allowing for the concept of electronic storage. This updated approach was the beginning of what is now called electronic disclosure. The procedure includes rules for determining the list of evidence, providing it to the parties, storage and sanctions for violating these rules. Given the increased risk of destruction of electronic evidence, the only legal deterrent to prevent this risk is the imposition of sanctions, which depend only on the discretion of the trial judge and must be assessed on a case-by-case basis. Particular attention is paid to metadata, which allows to establish the origin of information, context, authenticity, reliability and many other details necessary for the correct evaluation of evidence. It should be borne in mind that some of the difficulties associated with electronic evidence in the context

of e-discovery relate to the possibility of using certain information (especially metadata) for judicial purposes. The prospect of using information in electronic form as evidence in court is the essence of electronic disclosure of evidence, but the rules of this process are different from those that apply when the court must analyze their admissibility.

Key words: electronic evidence, disclosure of evidence, U.S. civil procedure, U.S. civil procedure, digital evidence, ESI, electronically stored information.

Список використаних джерел:

1. Craig Ball. Beyond data about data: the litigator's guide to metadata. URL: http://www.craigball.com/metadataguide2011.pdf.
2. David F. Herr and JoLynn M. Markison. E-Discovery under the Minnesota Rules: Where We've Been, Where We Might Be Headed. *William Mitchell L. Rev.* 2014. Vol. 40. Iss. 2. Article 3. P. 330–406.
3. ELECTRONIC EVIDENCE IN THE CLOUD: CHALLENGES IN THE US SYSTEM. URL: https://www.academia.edu/16433379/Electronic_evidence_in_the_cloud_the_US_system.
4. Elektra Entertainment Group v. Does 1-9. No. 04 Civ. 2289 (RWS), 2004 U.S. Dist. LEXIS 23560 (S.D.N.Y. Sept. 7, 2004).
5. Eric Hibbard. Electronic discovery standardization. *Ave Maria Law Review*. 2014. Vol. 12. Iss. 2. P. 313–327.
6. Experian Information Solutions, Inc. v. I-Centrix, L.L.C. No. O4 C 4437, 2005 U.S. Dist. LEXIS 42868 (N.D. Ill. July 21, 2005).
7. John H. Beisner. Discovering a better way: the need for effective litigation reform. *Duke L.J.* 2010. No. 60. P. 547–557.
8. Serge Jorgensen. Convergence of forensics, ediscovery, security & law. *Ave Maria L. Rev.* 2014. Vol. 12. Iss. 2. P. 291–292.
9. Digital evidence in cloud computing systems / M. Taylor and others. *Computer Law & Security Review*. 2011. No. 26. P. 304–308.
10. Marc Goodman. Future crimes. 1st ed. Bantam Press, 2015. 246 p.
11. Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984).
12. Silvestri v. General Motors, 271 F.3d. 4th Cir. 2001. P. 583–591.
13. Steven W. Teppler. Testable reliability: a modernized approach to ESI admissibility. *Ave Maria L. Rev*. 2014. Vol. 12. Iss. 2. P. 213–217.
14. Suggested Protocol for Discovery of Electronically Stored Information ("ESI") in the United States District Court for the District of Maryland. URL: http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf.
15. An Electronic Discovery Primer / Susan Burke and others. *William Mitchell L. Rev*. 2014. Vol. 40. Iss. 2. P. 427–433.
16. The Sedona Conference Working Group. The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production. January 2004.
17. The Sedona Conference. Commentary on Protection of Privileged ESI. November 2014. Public Comment. Version 2.
18. W. Lawrence Wescott II. The Increasing Importance of Metadata in Electronic Discovery. *14 RICH. J.L. & TECH*. 2008. Vol. 14. Iss. 3. P. 14.
19. Williams v. Sprint / United Management Co. 230 F.R.D. 640 ; D. Kan, 2005.