УДК 347
DOI https://doi.org/10.32782/2524-0374/2022-10/38

ЗАГАЛЬНОТЕОРЕТИЧНІ ЗАСАДИ ЗАХИСТУ ПРАВ ТА ІНТЕРЕСІВ СУБ'ЄКТІВ ДОГОВІРНИХ ВІДНОСИН У СФЕРІ ТЕХНОЛОГІЙ ХМАРНИХ ОБЧИСЛЕНЬ

GENERAL THEORETICAL PRINCIPLES OF PROTECTION OF THE RIGHTS AND INTERESTS OF THE SUBJECTS OF CONTRACTUAL RELATIONS IN THE FIELD OF CLOUD COMPUTING TECHNOLOGIES

Євлахова Е.Р., аспірантка кафедри цивільного права № 1
Національний юридичний університет імені Ярослава Мудрого

Нові технології завжди приносять із собою нові можливості. Проблема у цьому, нові можливості розподіляються нерівномірно. Про нерівномірність та її слідство — нерівність написано і сказано багато, і тут немає сенсу повторюватися. В даний час проблеми вибору оптимального правового механізму регламентації інформаційних хмарних технологій набувають все більшого значення. У справжній роботі, втім, торкаються питання економічної нерівності: вони важливі, та їх вивченням займається економічна наука. Дане дослідження присвячене правової нерівності (тобто порушення рівності, балансу інтересів), викликаного фактичними, що утворилися, на противагу юридичним, можливостями сторін правовідносин. Українське законодавство, так само як і закордонне, поки не містить будь-якого спеціального законодавчого регулювання сфери хмарних обчислень, у зв'язку з чим до діяльності з використання хмарних обчислень до суб'єктів даних відносин застосовуються загальні положення та норми чинного законодавства (або безпосередньо або за аналогією) закону), які далеко не завжди пропонують рішення, що відповідають суті відносин, що виникають між хмарним провайдером та користувачем. На основі вивчення зарубіжного досвіду у статті розглядатимуться різні варіанти поєднання державного регулювання та саморегулювання. У роботі наводиться короткий огляд «хмарних» технологій, розкриваються причини їх актуальності на сьогоднішній день, розглядається існуюче регулювання правовідносин у сфері використання «хмарних» технологій, у тому числі норми цивільного законодавства, що застосовуються до даних правовідносин. У цій статті автор порушує проблему визначення правової сутності договорів, які укладаються між операторами хмарних мереж та їх клієнтами. Проводиться аналіз із низкою поіменованих видами договорів. Обґрунтовується необхідність закріплення власного нормативного регулювання «хмарних договорів» через захист інформації, що зберігається на «хмарах», від несумлінних дій операторів мереж хмар.

Ключові слова: технології хмарних обчислень, IT сфера, інформаційні системи.

New technologies always bring with them new opportunities. The problem is that new opportunities are distributed unevenly. A lot has been written and said about inequality and its consequence - inequality, and there is no point in repeating it here. Currently, the problems of choosing the optimal legal mechanism for the regulation of information cloud technologies are gaining more and more importance. The real work, however, touches on issues of economic inequality: they are important, and economic science deals with their study. This study is devoted to legal inequality (that is, violation of equality, balance of interests) caused by actual, as opposed to legal, opportunities of parties to legal relations. Ukrainian legislation, as well as foreign legislation, does not yet contain any special legislative regulation in the field of cloud computing, in connection with which the general provisions and norms of current legislation (or directly or by analogy) the law), which do not always offer solutions that correspond to the essence of the relationship between the cloud provider and the user. Based on the study of foreign experience, the article will consider various options for combining state regulation and self-regulation. The work provides a brief overview of "cloud" technologies, reveals the reasons for their relevance today, examines the existing regulation of legal relations in the field of using "cloud" technologies, including the norms of civil legislation applicable to these legal relations. In this article, the author raises the problem of determining the legal essence of contracts concluded between cloud network operators and their clients. The analysis is carried out with a number of named types of contracts. The necessity of establishing own regulatory regulation of "cloud contracts" through the protection of information stored in "clouds" against unscrupulous actions of cloud network operators is substantiated.

Key words: cloud computing technologies, IT sphere, information systems.

У 2006 р. один з найбільших інтернет-магазинів Amazon вперше запропонував широкому колу споживачів нову інтернет-послугу: надання клієнтам можливості використовувати обчислювальні ресурси, технічні пристрої та додатки для віддаленого зберігання даних і виконання операцій. З того часу світовий ринок загальнодоступних хмарних послуг (сервісів), за даними Gartner, зріс у 2017 р. до 246,8 млрд дол. % корпоративних угод з IT-аутсорсингу [1].

Хмарні послуги (обчислення) (cloud computing) є технологію (технологічну модель) віддаленого доступу до загального фонду конфігурованих обчислювальних комп'ютерних ресурсів (серверам, пристроям зберігання даних, мереж передачі, додаткам та інших.). Переваги технологічної моделі хмарних сервісів полягають у тому, що їхні споживачі, уникаючи власних витрат на створення та експлуатацію цифрових технологій та обладнання, використовують технологічні можливості провайдера: його технологічну інфраструктуру та обчислювальні потужності, які можуть адаптуватися залежно від потреб користувачів [2]. Крім того, хмарні сервіси відрізняють високу продуктивність та безпеку, а також еластичність архітектури, що є особливо важливим для корпоративних відносин. Хмарні послуги у поєднанні з технологіями блокчейн та іншими цифровими технологіями також набули широкого застосування в банківському секторі економіки, дистанційному навчанні, віддаленому наданні медичних послуг, IT-індустрії, індустрії комп'ютерних ігор, розваг, кіберспорту та ін.

Хмарні послуги сприяють формуванню сучасної цифрової екосистеми, а операційні можливості цих цифрових технологій можуть бути інструментом адаптації права до реалій цифрового світу. Досягнення у сфері хмарних технологій, баз даних та мобільних технологій зумовили перехід від автоматизації та застосування промислових роботів до штучного інтелекту як реального інструменту, здатного не тільки замінити людину в рутинній праці, а й скласти їй конкуренцію в інтелектуальній сфері. Розвиток цифрових технологій став чинником цифровізації права[3]. Глобалізація, розширення сфер транскордонного обороту товарів, послуг та капіталів у сукупності із застосуванням сучасних технологій в умовах цифрової екосистеми формують новий правовий ландшафт та розширюють сфери дії права інтелектуальної власності.

Хмарні сервіси є складними програмно-апаратними системами (платформами), які включають кілька структурних елементів: дата-центри (центри обробки даних, хмарні сховища даних) з мережним та серверним обладнанням, інтернет-каналами зв'язку; розподілені файлові системи з використанням апаратних та віртуальних засобів, засобів

шифрування та захисту; віртуальні операційні системи, ресурси та програми, а також веб-сервіс з ідентифікатором (веб-адресою). У хмарних сервісах застосовуються у різних комбінаціях спеціальні програми (NetSuite, Sales-force.com), платформи (Google App Engine, Windows Azure, Bluemix, Amazon SQS (S3), Heroku та ін.), інфраструктура (Amazon EC2, IBM Cloud, AmazonVPC та ін).

У свій час Національний інститут стандартів і технологій США (NIST) дав визначення поняття хмарних сервісів: це модель забезпечення повсюдного та зручного мережевого доступу на вимогу до обчислювальних ресурсних пулів (наприклад, мереж, серверів, систем зберігання, додатків , сервісів), які можуть бути оперативно надані або звільнені від навантаження з мінімальними зусиллями щодо управління та взаємодії з постачальником послуг [4].

У практиці хмарних технологій нерідко застосовується правова конструкція оренди серверних потужностей, додатків та засобів інтеграції, які має провайдер. Як приклад можна навести хмарну технологічну платформу Cloud Edition on Amazon EC2, що надає користувачам можливість брати програмне забезпечення компанії «Informatica» у погодинну аренду[5].

Як зазначають експерти[6], хмарні технології забезпечують віддалений доступ до таких сервісів: «Все як послуга» (EaaS); «Інфраструктура як послуга» (IaaS); «Платформа як послуга» (PaaS); «Бізнес-платформа як послуга» (BPaaS); «Програмне забезпечення як послуга» (SaaS); «Апаратне забезпечення як послуга» (HaaS); «Робоче місце як послуга» (WaaS); «Інформаційне забезпечення як послуга» (DaaS); «Безпека як послуга» (SecaaS). Найбільшого поширення набули сервіси IaaS, PaaS та SaaS. Відповідно до сервісу IaaS провайдер постачає два типи ресурсів: обчислювальні потужності (у тому числі ресурси мережі) та ресурси зберігання (ресурси пам'яті). Надання сервісу PaaS полягає в тому, що клієнт отримує платформу (додаткові сервери) або інструмент для розробки програмного забезпечення. Область застосування SaaS пов'язана з наданням послуг поштових серверів, редакторів документів, систем керування взаємовідносинами з клієнтами та ін. Як правило, BPaaS передбачає повну передачу процесу на аутсорсинг без участі співробітників компанії-споживача.

Хмарні послуги поділяються на приватні або закриті (для обмеженого кола осіб), публічні або відкриті (для необмеженого кола осіб), а також змішаного типу.

Стрімкий розвиток технологій сприяє появі та нових договірних конструкцій. Так, новим договором на надання хмарних сервісів (послуг) останніми роками став SLA (Service Level Agreement). Зважаючи на специфіку регульованих цими договорами відносин, що включають як приватно-правові (договірні) відносини, так і публічні (безпека, обробка персональних даних), SLA виділено в окрему групу сервісних договорів. Предмет SLA передбачає підключення клієнта до додатка постачальника (провайдера) хмарних сервісів, а хмарний провайдер приймає на себе зобов'язання щодо управління системою, моніторингу трафіку та потреб клієнтів, зберігання та обробки інформації в «хмарі».

До суттєвих умов SLA зазвичай відносять: визначення переліку видів та параметрів послуг; методологію моніторингу, включаючи характеристики та методику вимірювання параметрів безпеки в режимі реального часу; умови незалежного тестування; діапазони параметрів, які викликають попередження ad hoc, реагування на інциденти чи відновлення; регулярні звіти про рівень обслуговування та їх зміст; пороги реагування, що визначаються відповідно до профілю ризику організації; межі та підстави відповідальності сторін та санкції за порушення договірних зобов'язань. Особливо обумовлюються умови забезпечення безпеки та захисту інформації, контроль за діяльністю виконавця, захист прав інтелектуальної власності, а також порядок електронного документообігу та використання електронного підпису[7].

Тим не менш, SLA можуть мати свою специфіку в залежності від виду сервісу, що надається провайдером. Так, договір на сервісні послуги SaaS не відкидає можливості закріплення в ньому положень, властивих ліцензійним угодам щодо використання об'єктів інтелектуальної власності. Як зазначає А.І. Савельєв[8], це може бути пов'язано з наданням провайдером прав на використання інформації, що розміщується в «хмарі», яка зберігається на устаткуванні провайдера, або на застосування допоміжного програмного забезпечення (enabling software), яке клієнт встановлює локально для використання сервісу SaaS. Однак це додаткові (супутні) послуги, що входять до загального комплексу послуг сервісу, і вони не змінюють правову природу SLA.

Відповідно до таких програмних документів ЄС, як «Digital Agenda for Europe 2015» («Цифровий порядок денний для Європи»), «Single Digital Market» («Єдиний цифровий ринок»), «An Industrial Policy for the Globalization Era» (« Індустріальна політика в еру глобалізації», «The Innovation Union» («Інноваційний союз»), пріоритетами ЄС є розширення та покращення доступу до цифрових мереж, товарів та послуг, велика «оцифрованість» економіки, а також стандартизація у п'яти найбільш важливих технологічних галузях: 5G, хмарні технології, інтернет речей, інформаційні технології та кібербезпека.

Європейський Союз виявляє особливий інтерес до хмарних обчислень. У вересні 2012 р. Європейська комісія ухвалила стратегію «Розкриття потенціалу хмарних обчислень у Європі» (Unleashing the Potential of Cloud Computing in Europe)[8], яка стала результатом аналізу загальних політичних, нормативних та технологічних ландшафтів та заохочує використання хмарних обчислень у всіх секторах європейської економіки. У ній визначаються три ключові напрями: 1) безпечні та справедливі умови контрактів; 2) розчищення великої кількості («джунглів») стандартів у сфері хмарних обчислень; 3) створення європейського «хмарного партнерства».

Завдяки стандартизованим інтерфейсам, організованому супроводу інфраструктури та забезпеченню безпеки даних хмарні сервіси можуть бути використані підприємствами, включаючи державні структури замість внутрішніх центрів обробки даних, а також департаментів, відповідальних за інформаційно-комунікаційні технології. « Компанії без своїх вкладень у створення інформаційної інфраструктури можуть запропонувати майбутнім споживачам послуги та роботи « [9].

У розвиток Стратегії Комісії ЄС 2012 р. Європарламент ухвалив Резолюцію про розкриття потенціалу хмарних сервісів та технологій від 10 грудня 2013 р.[17], яка включала такі блоки питань: «хмара» як інструмент зростання та зайнятості; ринок ЄС та «хмара»; державні закупівлі та закупівлі інноваційних рішень та «хмара»; національні стандарти та «хмара»; права споживачів та «хмара»; інтелектуальна власність, цивільне право та інше законодавство та «хмара»; захист персональних даних та основних прав громадян та «хмара».

На додаток до загальноєвропейських директив та вказівок ЄС, які застосовуються до хмарних обчислень, країни ЄС ухвалили національні законодавчі акти щодо захисту даних та хмарних обчислень.

Наприклад, у Чехії в 2013 р. було прийнято Закон про захист персональних даних у хмарних сервісах, який включає: визначення термінів «хмарні обчислення», «IaaS», «SaaS», «PaaS», «публічна хмара», «приватна хмара» і «гібридна хмара»; визначення понять контролера даних та обробника даних; порядок оцінки адекватності рівня захисту; правила щодо передачі персональних даних за межі Чеської Республіки; роз'яснення стандарт-

них умов договорів щодо використання хмарних сервісів та обов'язкових корпоративних правил.

У Великобританії прийнято Стратегію цифрової економіки (Digital economy strategy) на період 2015 — 2018 рр., а в 2017 р. прийнято новий Закон про цифрову економіку (Digital Economy Act 2017), який замінює раніше чинний документ 2010 р. На додаток до встановленим у Законі про захист даних (Data Protection Act 1998), у 2012 р. було прийнято Звід керівних принципів для компаній з питань хмарних обчислень. У цьому акті, зокрема, передбачені вимоги до обробки інформації у хмарі (три основні типи моделей хмарного розгортання: приватні, публічні та змішані).

У країнах ЄС питання конфіденційності та захисту даних мають першорядне значення при використанні хмарних обчислень, і це логічно, оскільки надання послуг через Інтернет у багатьох випадках призводить до обробки персональних даних. Це створює проблеми, пов'язані з застосовним правом, визначенням регулятора і провайдера, їх правочинів, умов контрактів, що укладаються на хмарні сервіси і міжнародною передачею даних.

Основні правила здійснення хмарних обчислень, що діють на території Європейської економічної зони (ЄЕЗ), спочатку викладені у Директиві ЄС про захист даних 1995 р.[10], яка була замінена новим директивним документом ЄС — Загальноєвропейським регламентом захисту даних (GDPR)[11]] (набув чинності у 2018 р.). Він регулює питання захисту персональних даних та конфіденційності, експорту персональних даних за межі ЄС з метою встановлення контролю громадян та мешканців ЄС за своїми персональними даними, а також спрощення регуляторного середовища для міжнародного бізнесу шляхом уніфікації регулювання у межах ЄС. Відносини в Інтернет-просторі ЄС регламентуються також Директивою про конфіденційність та електронні засоби зв'язку — так званою Директивою ePrivacy (зі змінами, внесеними Директивою 2009/136/ЄС у 2013 р.)[12], яку планується істотно змінити, оскільки набрав чинності GDPR .

Директива ePrivacy є частиною нормативної бази всіх держав — членів ЄС та регулює електронні комунікації, обробку персональних даних та захист приватного життя у секторі електронних комунікацій. Правила, викладені в Директиві ePrivacy, поширюються лише на послуги, які кваліфікуються як послуги електронного зв'язку. Зокрема, Директива встановлює правила щодо зобов'язань щодо безпеки постачальниками послуг електронного зв'язку; конфіденційності електронних повідомлень та пов'язаних з ними даних про трафік; конфіденційності кінцевого обладнання електронного зв'язку; обробки даних про трафік; відправлення повідомлень, що не запитуються. Директива захисту даних та Директива ePrivacy доповнюють одна одну, оскільки обидві регламентують сферу електронних комунікацій. Директива захисту даних застосовується до всіх секторів, включаючи сектор електронних комунікацій, за умови, що це питання не регулюється lex specialis, встановленим Директивою ePrivacy[13].

Особливу категорію даних, до яких застосовується спеціальний правовий режим відповідно до Директиви ЄС про захист даних, становлять так звані конфіденційні дані. Обґрунтування посиленого правового режиму захисту таких даних базується на презумпції, що їх використання може мати серйозні наслідки для основних прав та свобод людини. Наприклад, неправильне використання медичних даних може бути необоротним.

Відповідно до Директиви ЄС про захист даних до конфіденційних даних відносяться особисті відомості, що розкривають расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, членство у профспілках, а також дані щодо здоров'я чи статевого життя.

Вимога забезпечення безпеки персональних даних та захисту їх цілісності є ключовою у європейському законодавстві, яке покладає на оператора обробки даних обов'язок вжити технічних та організаційних заходів, необхідних для захисту персональних даних від випадкового чи незаконного знищення, втрати, а також від зміни та будь-якої іншої несанкціонованої (в тому числі хакерської) обробки, включаючи випадки, коли обробка тягне за собою передачу даних по мережі Інтернет. Аналогічні положення щодо безпеки даних містяться в національних законах країн ЄС щодо захисту даних.

Крім того, крім національних органів країн ЄС, що займаються захистом даних, спеціальний орган ЄС — Європейське агентство мережевої та інформаційної безпеки (ENISA) — забезпечує розробку принципів та рекомендацій щодо інформаційної безпеки (включаючи захист від інцидентів та безпеку у хмарному середовищі), а також здійснює моніторинг їх застосування.

Актуальну проблему у сфері інформаційної безпеки країн ЄС становить аутентифікація учасників кіберпростору. Проблема пов'язана з анонімним або псевдонімним відображенням даних і завдячує своєю появою таким новим технологіям, як великі бази даних (big data), інтернет речей (IoT) та хмарні обчислення. Цілком природний інтерес до методів, які дозволять усунути або, принаймні, пом'якшити ризики щодо обробки персональних даних при використанні таких технологій[14].

Директива ЄС про захист даних визначила основні принципи захисту даних, які повинні застосовуватися до будь-якої інформації щодо ідентифікованої або ідентифікованої особи, а також враховувати всі засоби, які можуть бути розумно використані оператором даних або будь-яким іншим суб'єктом для ідентифікації зазначеної особи[15].

Стаття 6 (1) Директиви ЄС про захист даних вимагає, щоб інформація зберігалася не довше, ніж це необхідно для цілей, для яких дані були зібрані або для яких вони обробляються у формі, що допускає ідентифікацію. Для дотримання зазначених норм можна використовувати анонімізація[16].

У Франції та Сполученому Королівстві прийнято спеціальні посібники із застосування положень про захист даних. Зокрема, Управління комісара з інформації (Information Commissioner's Office, ICO) Великобританії опублікувало зведення практичних правил управління ризиками, пов'язані з анонімізацією[17]. Звід містить механізм, що дозволяє оцінити ризики анонімізації, пов'язані із захистом даних та ідентифікацією фізичних осіб, включає приклади того, як може бути досягнуто успішної анонімізації (зокрема, особисті дані можуть бути анонімізовані для медичних досліджень). ICO також оголосило, що консорціум, очолюваний Манчестерським університетом, разом з університетом Саутгемптона, Управлінням національної статистики та новим Інститутом відкритих даних керуватимуть новою британською мережею анонімізації (UKAN), яка дозволить обмінюватися передовою практикою, пов'язаною з анонімізацією, в державному секторі.

Хмарні технології (обчислення, сервіси) набули широкого поширення завдяки своїй надійності, безпеці та доступності. Проте зростаючу конкуренцію хмарним сервісам становлять технологічні платформи з урахуванням розподіленого реєстру (блокчейн-технології), створювані такими великими IT-компаніями, як Apple і Google.

Хмарні технології є елементами цифрової економіки, що формується, і технологічної інфраструктури цифрової екосистеми в цілому, що дозволяє говорити про виділення нового правового інституту цифрових послуг. Нещодавнє перетворення Мінкомзв'язку в Міністерство цифрового розвитку, зв'язку та масових комунікацій підтверджує важливість координації та системного підходу до розвитку в країні цифрових технологій та вдосконалення законодавчої бази у цій сфері.

ЛІТЕРАТУРА

1. Аубакіров М. З., Нікульчев Є. В. Завдання розробки хмарних платформ задля забезпечення інформаційних потреб державного сектора. Київ, 2015. URL: https://cloudofscience.ru/publications/archive/cos_2_2
2. Карцхія А.А. Цифровізація у праві та правозастосуванні. *Моніторинг правозастосування.* 2018.
3. Карцхія А. А. Цифрове майбутнє класичної цивілістики. *Моніторинг правозастосування.* 2018.
4. Понкін І.В., Редькіна А.І. Штучний інтелект право інтелектуальної власності. *Інтелектуальне право. Авторське право та суміжні права.* 2018. № 2.
5. Савельєв А.І. Правова природа «хмарних» сервісів: свобода договору, авторське право та високі технології. *Вестн. громадян. права.* 2015. № 5.
6. Черняк Л. Інтеграція - основа хмари. *Відкриті системи.* 2011. URL: https://www.osp.ru/os/2011/07/13010473
7. Ентін В.Л. Авторське право у віртуальній реальності (нові можливості та виклики цифрової епохи). 2017.
8. Муравський В. В. Комп'ютерно-комунікаційна форма обліку. 2018.
9. Сало Н. М. Інформаційно-комунікаційні технології в контексті сучасних міжнародних відносин. 2017.
10. Іншакова А. О. Право та інформаційно-технологічні перетворення суспільних відносин в умовах індустрії 4. 0. *Legal Concept.* 2019. Т. 18, № 4. С. 6–17.
11. Іншакова А. О. Право як основа інфраструктурного забезпечення цифрової економіки та технології інтернету речей. *Legal Concept.* 2019. Т. 18, № 3. С. 6–11.
12. Близнюк І. А. Цивільно-правова модель регулювання цифрових технологій. С. 394.
13. Дмитрик Н. А. Цифрова трансформація: правовий вимір. Правознавство. 2019. Т. 63, № 1. С. 28–46.
14. Полякова Т. А., Хімченко А. І. Цифрова трансформація: правовий вимір. *Правознавство.* 2019. Т. 63, № 1. С. 28–46.
15. Нікуліна О. В., Кізім А. А. Хмарні технології як модель впровадження інновацій. *Наука та освіта: господарство та економіка; підприємництво; право та управління.* 2014. С. 12–19.
16. Касаткін П. А. Хмарні обчислення - майбутнє світового ринку інформаційних технологій. *Науково-методичний електронний журнал Концепт*. 2016. Т. 34. С. 138–145.
17. Дуккардт А. Н., Саєнко Д. С., Слєпцова Є. А. Хмарні технології в освіті. *Відкрита освіта*. 2014. № 3. С. 68–74.