Міністерство освіти і науки України

Національний університет «Києво-Могилянська академія»

Факультет правничих наук

Кафедра приватного права

Магістерська робота

Освітній ступінь — магістр

На тему: **«Правове регулювання хмарних послуг: світові та українські тенденції»**

«Legal regulation of cloud services: global and Ukrainian trends»

Виконав: студент 2 р. н.
магістерської програми «Право»
факультету правничих наук
Петренко Михайло Анатолійович

Керівник Посполітак Володимир Володимирович
доцент, кандидат юридичних наук

Рецензент

Магістерська робота захищена
з оцінкою _____
Секретар ЕК _____
«__» _____ 2024 р.

Київ-2024

Декларація
академічної доброчесності

Я, Пєріенко Михайло Анатолійович, студент 2 року навчання магістерської програми за спеціальністю 081 "Право" ФПВН НаУКМА підтверджую таке:

- написана мною магістерська робота на тему "Правове регулювання хмарних послуг (світовий та український досвід)" відповідає вимогам академічної доброчесності та не містить порушень передбачених п. 3.1 Положення про академічну доброчесність здобувачів освіти у НаУКМА, з'ясованого мною ознайомлений

08.05.2024

Пєріенко М.А.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

IaaS	- Інфраструктура як послуга
PaaS	- Платформа як послуга
SaaS	- Програмне забезпечення як послуга
GDPR	- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
ЄС	- Європейський Союз
NIS 2	- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union
DSA	- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
DMA	- Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)
КУпАП	- Кодекс України про адміністративні правопорушення
НАТО	- Організація Північноатлантичного договору
США	- Сполучені Штати Америки

ВСТУП

Тема магістерської роботи: «Правове регулювання хмарних послуг: світові та українські тенденції»

Актуальність теми: В наш час все більше та більше споживачів, підприємств, організацій та публічних інституцій покладаються на зберігання даних в хмарних сервісах. Зокрема, дослідження за участю 753 технічних і бізнес-професіоналів по всьому світі виявило, що з них 63 відсотки широко використовують хмару у своїй діяльності, а загалом принаймні однією хмарною службою користується 3.6 мільярдів користувачів у світі. [99]

Це загалом призводить до того, що індустрія хмарних послуг стає невід'ємною частиною суспільного життя та економічних процесів. Водночас, така велика залежність суспільства від хмарних послуг створює і деякі ризики, які потребують дослідження для подальшого попередження, в тому числі правовими і регуляторними способами. Зокрема, критично важливо, щоб хмари забезпечували доступ до даних лише авторизованим особам та зберігали їх у належному вигляді. Масштабні порушення цих зобов'язань можуть мати дестабілізуючі наслідки, через що деякі країни навіть розробляють доктрину хмарного суверенітету. [100]

Подібне зростання значення хмарних послуг і потенційних ризиків, відбувається на фоні того, що приватні особи значною мірою довіряють хмарам, часто не розуміючи принципи їх роботи та розподілу прав і обов'язків. Fide, sed cui, vide. Однак, диспозитивний контроль у відносинах з великими хмарними провайдерами ускладнений через фактичну нерівноправність сторін. Тому важливим стає встановлене правове регулювання, яке є імперативним для хмарних провайдерів.

В сукупності названі фактори свідчать про необхідність розвитку продуманої правової політики для в контексті хмарних послуг. Як зазначала Музика Л. А. у своїй монографії, метод цивільно-правової політики є комплексним, а не тільки диспозитивним, а основним суб'єктом імперативних

відносин в межах такої є держава, в них вона домінує, а не виступає як рівний суб'єкт на кшталт її участі у цивільно-правових відносинах. [101; с. 491]

Відповідно, у цій роботі я фокусуюся на тому, аби описати тенденції розвитку правової політики і загалом правового регулювання, які є ключовими для попередження основних ризиків, що виникають через все більшу роль хмарних послуг у суспільному житті.

Об'єктом дослідження є суспільні відносини, які виникають в процесі надання хмарних послуг, переважно в Європейському Союзі та Україні.

Предметом дослідження є теоретичні дослідження на тему характеристики та проблематики правового регулювання хмарних послуг, захисту персональних даних, безпеки даних, захисту прав споживачів та цифрової конкуренції в контексті хмарних послуг, нормативні акти ЄС та України, їх конкретні норми, правозастосовна (в тому числі судова) практика, що дотичні до відносин хмарних послуг, очікувані зміни до таких актів, та їх взаємовплив з сучасним ринком та наявною практикою (переважно нішових світових провайдерів таких) надання хмарних послуг.

Дослідницьке питання дослідження поставлено так: «Які існують наразі тенденції правового регулювання хмарних послуг та яке їх значення?»

Метою дослідження є здійснення огляду та характеристики наявної та очікуваної правової політики, а також конкретних актів щодо предмету регулювання відносин, які виникають при наданні хмарних послуг.

Для розкриття поставленої мети були сформовані такі ***завдання дослідження:***

- визначити правову природу хмарних послуг, їх характеристику як явища у суспільстві, кон'юнктуру ринку та виклики, які виникають у сучасній практиці їх надання;
- дослідити вплив правового регулювання захисту персональних даних та захисту інформації Європейського Союзу на надання хмарних послуг;
- дослідити вплив правового регулювання захисту цифрової конкуренції та прав споживачів у Європейському Союзі на надання хмарних послуг;

- дослідити особливості правового регулювання хмарних послуг відносин в Україні.

Теоретичною базою дослідження були праці правових дослідників Мішеля Й., Мілларда К., Тертон Ф., Куан Хон В., Сінгв Дж., Бенолієля У., Бехера С., Камарін Д., Уолдена Я., Біла Г., Міклица Х.-В., Райха Н., Форе М., Віссхера Л., Манганеллі А., Євлахової Е., Давидової Н., Ходико Ю., Коверзнєва В., Пономарьова С., Іванова А. та інших.

Емпіричну базу дослідження становлять опитування користувачів щодо практики використання хмарних послуг, нормативні та інші акти Європейського Союзу, закони України, підзаконні акти України, матеріали судової практики України та іноземних судів.

Методологія дослідження включає застосування переважно аксіологічного, діалектичного, аналітичного, формально-юридичного, порівняльно-правового методів та методу правового моделювання.

Аксіологічний метод застосовувався для визначення фундаментального значення прав користувачів хмарних послуг, *діалектичний* — для визначення підходів до правозастосування галузевих норм в контексті хмарних послуг, *аналітичний* — повсюдно для виокремлення окремих аспектів ширших норм та понять для цілей регулювання хмарних послуг тощо, *формально-юридичний* — для роботи з правовими нормами у різних розділах роботи, *порівняльно-правовий* — для порівняння правових норм у всіх розділах, *метод правового моделювання* — переважно для формулювання правових тенденцій на підставі наявних практик регулювання та інших елементів дослідження.

РОЗДІЛ 1
ПРАВОВА ПРИРОДА ХМАРНИХ ПОСЛУГ ТА ВИКЛИКИ ЇХ ПРАВОВОГО РЕГУЛЮВАННЯ

1.1. Правова природа хмарних послуг

Для здійснення ефективного дослідження стану і тенденцій правового регулювання хмарних послуг варто передусім окреслити правову природу хмарних послуг як таких.

Центральним елементом хмарних послуг та об'єктом навколо якого вибудовуються ці відносини, є модель хмарних обчислень (cloud computing). Загальноприйняте визначенням хмарних обчислення загалом сформульоване Національним інститутом стандартів і технологій США (NIST):

«модель забезпечення повсюдного та зручного доступу на вимогу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та взаємодіями з провайдерами.» [7]

Також, визначенням безпосередньо хмарної послуги може слугувати дане в Директиві ЄС № 2022/2555:

«"послуга хмарних обчислень" означає цифрову послугу, яка забезпечує адміністрування на вимогу та широкий віддалений доступ до масштабованого та еластичного пулу спільних обчислювальних ресурсів, включаючи випадки, коли такі ресурси розподілені між кількома місцями;» [48; ст. 6(30)]

Без занурення у кожен аспект визначень, слід акцентувати увагу на ключових характеристиках, які відрізняють хмарні послуги від інших видів цифрових послуг і які будуть впливати на їхнє особливе правове регулювання:

1. Провайдери хмарних сервісів пропонують доступ до своїх обчислювальних потужностей, а саме серверів, що зберігають або обробляють інформацію користувачів. Це означає, що користувачі передають свої дані для зберігання провайдеру.

2. Користувачі мають безперервний та необмежений доступ до своїх даних на серверах за власною вимогою.

3. Процеси завантаження та видалення інформації з хмарних серверів повинні бути простими та не вимагати значних зусиль з боку користувача, наприклад, без необхідності особистого звернення до провайдера, завдяки легкодоступному функціоналу.

Також, важливим для цілей регулювання й здійснити правильну класифікацію хмарних послуг, адже існує надто широкий спектр таких, що передбачає й різний зміст правовідносин. Зокрема, важливим є поділ на підставі розподілу міри контролю над хмарою між користувачем та хмарним провайдером. В межах цього поділу виділяють наступні типи хмарних послуг:

1. Інфраструктура як послуга (IaaS), коли постачальник просто надає віддалений доступ і використання фізичних обчислювальних ресурсів, а користувач відповідає за впровадження та підтримку як операційної платформи, так і всіх додатків. [8; с. 194]

2. Платформа як послуга (PaaS), коли постачальник надає доступ і використання операційних платформ, а також базового обладнання, але користувач залишається відповідальним за впровадження та підтримку додатків. [8; с. 194]

3. Програмне забезпечення як послуга (SaaS), де постачальник надає інфраструктуру, платформу та додаток, а користувач лиш надає власні дані на зберігання та/або обробку через цей додаток. [8; с. 194]

Загалом, IaaS є типом хмари, де користувач має найбільшу гнучкість, адже може розгортати повністю свої операційні системи, програми і встановлювати власні правила управління такими, а його контроль над хмарними потужностями є найповнішим, що водночас збільшує і його сферу відповідальності, адже надавач хмарних послуг відповідальний переважно тільки за апаратно-технічне забезпечення. Водночас, SaaS є платформою, яка надає найбільшу сферу контролю саме хмарному провайдеру, як водночас і майже всі ризики, які він несе; користувач же в такому випадку, програючи в гнучкості і кастомізації,

виграє в зручності і відсутності необхідності самостійного створення додатків, тому більшість хмарних додатків, що використовуються людьми в персональних цілях (як-от електронна пошта) є хмарами типу SaaS. [9]

Однак в розрізі різних типів хмарних послуг варто зауважити, що не виключається, що хмарних провайдер, який надає послуги SaaS-типу використовує для зберігання своїх даних PaaS чи IaaS хмару. В такому випадку, ситуація із суб'єктами відносин хмарних послуг є більш складною, ніж прості відносини послуг між надавачем і отримувачем. Варто підкреслити, що на практиці такі випадки трапляються досить часто: клієнт, який укладає контракт із постачальником хмарних послуг, не є кінцевим споживачем цих послуг. Наприклад, платформа музичного стримінгу Spotify, будучи клієнтом Google Cloud, використовує ці хмарні ресурси для обслуговування власних користувачів. [10] Загалом, таке явище називають розшаруванням (layering) хмарних сервісів. [26; с. 6] Ба більше, ці ускладнення можуть формувати складні системи ланцюжків між хмарами, які можуть виступати клієнтами один одного, аби ефективно зберігати дані кінцевих користувачів. [14; с. 26-30]

Загалом, описане явище може призводити до складнощів в тому питанні, хто саме відповідальний перед користувачем у разі порушення його прав при наданні його послуг і чи договірний розподіл ризиків між такими двома надавачами хмарних послуг не обмежить користувача в очікуваній можливості захисту власних прав.

Окремим аспектом, який варто розглянути є місце хмарних послуг серед цивільно-правових договорів українського законодавства. Це питання варто розглянути через сутність хмарних послуг, щодо якої повного консенсусу в дослідників ще немає.

Як зазначає Євлахова Е. Р. у доктрині договір хмарних послуг окрім власне договору про надання послуг, інколи розглядають як договір оренди чи договір зберігання. [79; с. 20-21] Таку думку можна пояснити тим, що загалом з певної технічної точки зору, хмарні послуги передбачають собою надання серверів для зберігання даних іншої особи, які вона «орендує» чи дає на «зберігання».

Водночас, більшість дослідників критикує таку точку зору. Зокрема Давидова Н. оцінюючи договір хмарних послуг як договір оренди програмно-апаратного комплексу зазначає, що:

«У договорі оренди програмно-апаратного комплексу про «оренду» можна говорити лише в економічному розумінні – як про оплатне користування чужим майном, але не як про правову категорію. З точки зору українського законодавства хмарний сервіс являє собою інформаційну систему, яка включає сукупність технічних засобів, інформацію та програмне забезпечення, що відповідає за обробку даних. Головною проблемою застосування до вказаних відносин конструкції договору найму (оренди) є те, що ЦК України відносить до предмета договору найму лише неспоживну річ, тобто ту, яка визначена індивідуальними ознаками і яка зберігає свій первісний вигляд при неодноразовому використанні (ч. 1 ст. 760 ЦК України). Сукупність серверів, яка використовується для хмарного сервісу, не може бути індивідуалізовано, програмне забезпечення також не є неспоживною індивідуально визначеною річчю. Більш того, одним і тим самим сервером можуть одночасно користуватися десятки тисяч клієнтів, що робить технічно та юридично неможливим виокремити предмет договору для кожного з них. Договір оренди програмноапаратного комплексу може бути визнаний нікчемним, оскільки суперечить вимогам норм ЦК України.» [80; с. 19]

З цією думкою можна погодитися, звернувши увагу на два основні аспекти. По-перше, дійсно як зазначається, категорія оренди в українському законодавстві є фактично не застосовною до програмно-апаратного обладнання, яке власне і становить хмару. По-друге, як зазначалося, хмарний провайдер в обов’язках має набагато більше, ніж надати право використовувати відповідний сервер, а навпаки центральним елементом є не надання конкретного серверу, а скоріш та вигода, яку користувач отримує — програмне забезпечення чи платформа, яка часто оцінюється здатністю користувача надавати і отримувати дані та програми через неї. Фактичне знаходження такого серверу (окрім цілей вимог про захист персональних даних, однак це вже додатковий аспект комплаєнсу, а не первинний інтерес сторони), того чи фрагментуються між різними серверами тощо і яким чином і як часто між ними передаються загалом не є вагомим для сторони користувача, що ніяк не збігається зі сутністю оренди.

Також можна погодитися з думкою Давидової Н. щодо неможливості класифікувати хмарні послуги як договір зберігання:

«Відносини зберігання є елементом SaaS, але не охоплюють всіх аспектів цього комплексного явища. Згідно з класичним договором зберігання одна сторона (зберігач) зобов'язується зберігати річ, яка передана їй другою стороною (поклажодавцем), і повернути її поклажодавцеві у схоронності (ст. 936 ЦК України). Договір зберігання в розумінні глави 66 ЦК України обмежує об'єкт договору зберігання лише речами, тобто предметами матеріального світу, натомість у моделі SaaS йдеться про віртуальне зберігання цифрової інформації.» [80; с. 20]

Дійсно, об'єкт договору зберігання не можна застосувати наразі щодо інформації.

Також, на мій погляд треба розрізнити хмарні послуги від договорів підряду та ліцензійного договору.

Стосовно першого, варто зауважити, що важливою характеристикою договору підряду є те, що результат робіт це є «одномоментним» об'єктом зобов'язальних правовідносин, оскільки упродовж існування всього зобов'язального правовідношення він проходить стадію формування, створення, а після досягнення кінцевого, зумовленого сторонами результату трансформується в інший об'єкт, як правило, річ. [81; с. 141] Однак хмарні послуги не створюють кінцевого об'єкту, а полягають в тому, аби надавати постійний доступ до обчислювальних ресурсів, який при розірванні договору не зберігається, а існує тільки в процесі надання.

Зрештою, ліцензійний договір передбачає надання права використання об'єкта права інтелектуальної власності. [82; ст. 1109(1)] Водночас, хмарні послуги надають не право використання інтелектуальної власності, а доступ до сукупних обчислювальних ресурсів, що загалом не є інтелектуальною власністю. Втім, найбільш граничним моментом є договори типу SaaS, де програмне забезпечення, що надається провайдером може бути об'єктом інтелектальної власності. Давидової Н. щодо цього зазначає, що:

«Правове оформлення вказаних суспільних відносин зазвичай на практиці відбувається за допомогою ліцензійного договору, але такий підхід викликає сумнів з ряду причин, насамперед тому, що велику частку наведених суспільних відносин займає саме надання провайдером інформаційних послуг замовнику. По-друге, SaaS не є традиційною ліцензійною

угодою, як у разі купівлі примірника програми, що встановлюється на жорсткий диск комп'ютера користувача. Доцільніше кваліфікувати SaaS як підписку на доступ до програмного забезпечення. По-третє, питання якості комп'ютерної програми врегульовується договором про надання послуг і не може бути врегульовано в межах ліцензійного договору, оскільки предметом ліцензії є дозвіл (невиключне право), який не має властивостей речі чи послуги, тому не може бути оцінений за критерієм якості» [80; с. 20]

Зрештою, можна зазначити, що навіть якщо хмарний договір типу SaaS і передбачає ліцензію, то така не є основним елементом, що визначає цей договір як хмарний, а скоріш є додатковою умовою договору, яка додатково захищає права інтелектуальної власності надавача послуг.

Зрештою, дослідниця підходить до висновку, що

«найбільш оптимальною договірною конструкцією для врегулювання суспільних відносин SaaS в українському правовому середовищі є договір про надання послуг, у тому числі інформаційних послуг доступу до онлайн-сервісу.» [80; с. 21]

З цим можна погодитися, адже договір про надання послуг є дуже гнучким щодо предмету, якщо такий пов'язаний з тривалими відносинами у цифровій сфері, що дає можливість застосувати його щодо хмарного договору, адже як було досліджено, він може включати дуже багато різноманітних сервісів, які складно чітко описати через речові інститути чи інститути інтелектуальної власності.

Окрім цього, таку думку можна вважати такою, яка прийнята законодавцем у законі України «Про хмарні послуги», де вказано, що «хмарна послуга - послуга з надання хмарних ресурсів за допомогою технології хмарних обчислень;» [83; ст. 2(1)]

Відповідно, до хмарних послуг застосовується глава 63 Цивільного кодексу України, з особливостями, які передбачені в інших актах законодавства, зокрема у згаданому Закону України «Про хмарні послуги» передбачається обов'язкова письмова форма договору (зокрема, електронна), а також можливість договору включати положення, що посилаються на інші електронні документи. [83; ст. 10(1)]

В контексті вищезгаданого розшарування хмарних послуг варто зауважити, що таке в межах цивільного законодавства України буде оформлюватися кількома договорами про надання послуг: між провайдером та користувачем та провайдером з іншими провайдерами. Водночас варто зауважити, що оскільки статтею 902 Цивільного кодексу України передбачено особисте виконання договору виконавцем, якщо інше не передбачено договором, [82; ст. 902] то можливість передачі даних на зберігання третім сторонам має бути перебачено в договорі між користувачем і первинним провайдером.

1.2. Виклики правового регулювання хмарних послуг

Підґрунтям тенденцій і потенційного вектору руху правового регулювання будь-якого предмету є сучасні виклики, які постають перед суспільством щодо такого предмету. Саме тому, важливо здійснити огляд викликів, які постають перед правовим регулюванням хмарних послуг.

Характеризуючи такі, варто розпочати з того, що центральною ознакою хмарних послуг як явища у суспільстві є стрімкий їх розвиток та проникнення у різні сфери життя — від найбільших державних і суспільних інституцій, які використовують такі в стратегічних цілях, до окремо взятих людей, які зберігають особисті документи та записи у хмарі. Звісно, чим більший масштаб проникнення певного явища у суспільне життя, тим більше суспільство залежне від цього явища і відтак потребує кращого і системнішого його врегулювання. Тож важливо оглянути і оцінити масштаби використання хмарних послуг у сучасному світі.

Відповідно до актуальної статистики 94% компаній по всьому світу використовує хмару в тому чи іншому вигляді. Це число за останні 3 роки зросло на 14%. Майже половину даних, які зберігають компанії вони розцінюють як конфіденційні, а загалом компанії зберігають 60% власних даних на хмарі. Що стосується особистого використання, то 65,28% людей використовують персональне хмарне сховище як основне сховище даних. [1] [2] [3]

Водночас, 45% компаній в межах ЄС передплачують хмарні послуги, для малого бізнесу цей показник становить 41%, коли для середнього 59%. В межах цих компаній, що передплачують хмарні послуги, 77,4 % і 74,2 % відповідно середніх і малих компаній зазначали, що їх бізнес «надзвичайно залежний» від цих хмарних послуг. [4]

Загалом, ці статистичні дані свідчать про те, що хмарні послуги є фактично невід'ємною складовою як для бізнесу будь-яких розмірів так і для задоволення персональних цілей людей. Також, дана статистика говорить, що частина бізнесу використовує не тільки безоплатні хмарні рішення, а й передплачує їх, і більшість з таких компаній є надзвичайно залежні від отримання даних послуг.

Для оцінки кон'юнктури, в якій виникають відносини при наданні хмарних послуг, необхідно окрім отримувача хмарних послуг оцінити через ринкову призму й іншу сторону — надавача послуг.

Загалом, характеризуючи сучасний стан ринку надавачів хмарних послуг, варто зауважити, що 65% всього обсягу цих послуг здійснюється трьома компаніями — Amazon Web Services (AWS) (32%), Microsoft Azure (23%) та Google Cloud (10%). Водночас на 10 найбільших компаній з надання хмарних послуг припадає чотири п'ятих всього ринку. Річний дохід майже всіх цих компаній складає мільярди, а то й десятки мільярдів доларів. [5] [6]

В межах цих даних, можна підсумувати, що висока залежність великої кількості і різних типів споживачів від хмарних послуг з одного боку, і водночас домінування кількох великих компаній-провайдерів з іншого, призводить до переважної нерівномірності у договірних відносинах при наданні хмарних послуг. Це вказує на підвищене значення правового регулювання для цієї сфери, яке дозволить забезпечити більш справедливі та прозорі правила гри для всіх учасників ринку хмарних послуг, виправивши вади ринкової нерівності.

Водночас, запровадження правового регулювання у сфері хмарних послуг має відбуватися на засадах пропорційності та об'єктивної необхідності, уникаючи надмірного втручання у принцип свободи договору. Відповідно, замість запровадження універсального обтяжливого регулювання доцільнішим є

скоріш точковий підхід, зосереджений на вирішенні конкретних проблемних питань, що виникають внаслідок нерівного становища сторін та інших чинників. Тільки такий виважений підхід дозволяє мінімізувати організаційне та економічне навантаження на учасників відносин без належних на те підстав.

Водночас, в контексті попереднього питання варто зауважити, що загалом, договори про надання хмарних послуг між клієнтом та надавачем навряд чи забезпечують такий самий договірний захист, як договори про аутсорсинг чи багато інших договорів у цифровій сфері, навіть якщо клієнтом є не людина, а компанія чи організація. Клієнт, швидше за все, має менше важелів впливу на переговори, зокрема враховуючи і вищеописану ринкову диспропорцію. [11] І загалом, якщо говорити про людей, а також малий та середній бізнес, то вони можуть укласти договір хмарних послуг з майже будь-якими хмарними провайдерами тільки на основі стандартних договорів, які не підлягають обговоренню, текст яких складається виключно провайдерами та які укладаються методом "click-through". [14; с. 33] Це сукупно дає можливість зробити висновок, що дійсно ті ризики для клієнта, які можуть виникнути через особливість системи хмарних обчислень, хмарних послуг і способів їх надання, навряд будуть належно покриватися положеннями договору між клієнтом і постачальником послуг.

Ця думка також підтверджується і емпіричним дослідженням від 2019 року Школи права Лондонського університету королеви Марії, в якому аналізувалися стандартні умови 40-ка договорів про надання хмарних послуг від 32 з одних з найбільших надавачів хмарних послуг у світі. Загалом, багато провайдерів передбачає низку прав для себе як-от на одностороннє розірвання договору, право односторонньо змінювати умови надання хмарних послуг, повну або дуже широку відмову від відповідальності за будь-які збитки завданні порушеннями з боку надавачів тощо, водночас права користувачів часто обмежені (хоча деякі як право односторонньо розірвати договір зі свого боку збережені), не уточнені (як-от право на отримання своїх даних у разі розірвання договору) і, ба більше, часто самі послуги подаються у вигляді «як є». [12; с. 26-29, 30-33, 36, 42-44, 47-52]

Окремо варто виділити в контексті умов договору, що притаманні контрактам між хмарними провайдерами та їх клієнтами, що є фізичними особами, регулювання питання успадкування даних (в тому числі облікового запису і тд.) клієнта. Воно зокрема розглядалося в іншому дослідженні Школи права Лондонського університету королеви Марії від 2018 року: відповідно до нього переважна більшість хмарних сервісів не прописує в своїх стандартних положеннях те, що відбуватиметься з даними після смерті власника облікового запису. Решта або повністю виключають можливість спадкування або надають можливість призначити наслідника попередньо особисто власником облікового запису. Також в багатьох юрисдикціях дані на хмарі не розглядаються ніяким видом власності, аби на них поширювалися законні норми про спадкування чи навіть заповіт (особливо, якщо він безпосередньо не прописує долю облікового запису, а визначає загальну сукупність спадщини) [13; с. 15-16]

Водночас, незважаючи на те, що дані не завжди є майном у класичному розумінні, вони можуть мати значну цінність для спадкоємців померлої особи, зокрема моральну. Однак відсутність положень про їх спадкування як в стандартних умовах договору, так і відсутність дії щодо таких класичних законних положень є нагальною проблемою. Тут варто зважати на те, що деякі дані є вкрай персоналізованими та можуть містити конфіденційну інформацію, поширення якої могло б суперечити волі померлого власника облікового запису. Через це просте застосування норм про спадкування до цифрових даних є проблематичним і потребує виваженого підходу. Отже, врегулювання питання успадкування даних у хмарних сервісах вимагає ретельного аналізу та балансування різних інтересів – прав спадкоємців, волі померлого власника та фактичної можливості хмарі запровадити систему, яка запровадить належну процедуру сприяння вирішенню цього питання (а як ми бачимо з емпіричних даних, хмарні сервіси рідко задаються цим питанням). Відтак, на мою думку, варто розробити чітке регулювання того, як визначати процедури та умови успадкування даних хмари з урахуванням відповідних прав та інтересів усіх задіяних сторін.

Наступним викликом, який виникає з природи хмарних послуг є виклик суверенітету та локалізації даних. Тут важливим моментом є те, що найбільші провайдери, які, як було згадано вище, є нішовими на ринку, здійснюють свою діяльність всесвітньо. В силу технічних особливостей, для раціонального розподілу хмарних ресурсів та інших елементів ефективної роботи вони зберігають дані не на визначеному сервері, а постійно змінюють своє фактичне місце зберігання, часто ділячись, дублюючись, здійснюючи кешування тощо. Загалом ця застосовна технологія називається фрагментацією даних. І напевне ключовий правовий ризик неї є те, що один набір даних від одного клієнта зберігається на різних фізичних серверах, що можуть знаходитися в різних географічних регіонах. [14; с. 15-17] Цей факт також часто піднімає питання про застосування правових наслідків перетину даними кордону, адже відповідні норми (зокрема, щодо захисту персональних даних) часто застосовуються для конкретної усвідомленої передачі, а технічний рух частин і кешувань даних може бути надто ускладнений відповідними нормами. З іншого боку, передача даних закордон якою вона не була б, завжди несе ризики з точки зору захисту персональних даних і потребує регулювання, що буде розглянуто в наступних розділах цієї роботи.

Хоч вище було вже зазначено, що через ряд обставин, договори про надання хмарних послуг є такими, що зачасту дають слабкі гарантії клієнтам, однак варто розглянути детальніше ті конкретні ризикові елементи договорів, аби мати більш детальний фундамент для аналізу їх з точки зору правового регулювання, яке може їх вирішити.

Перша така обставина виникає навіть до укладення договору, адже ознайомлення зі стандартними умовами користування, що запропоновані користувачу, і які фактично є договором про надання послуг вже має істотні ризики через свою форму. Велике емпіричне дослідження від представників Бостонської школи права щодо складності текстів політик низки веб-сайти, частина з яких є хмарними провайдерами показало, що складність цих текстів таких можна порівняти зі складністю академічних статей, що є абсолютно не

орієнтованим на звичайного клієнта, дивлячись, що такими можуть бути звичайні споживачі чи представники мікро-бізнесу, яким юридичні послуги навряд будуть доступні щодо даного питання. [15; с. 2256-2259] Це загалом призводить до того, що в середньому лише 1% людей читають подібні положення, які надаються на ознайомлення в тому числі хмарними сервісами. [16] Як наслідок, навіть не маючи можливість вплинути на умови договору про надання хмарних послуг, споживачі де-факто часто не мають можливості й ознайомитися з ними.

Іншою обставиною, що ще більше ускладнює поінформованість споживача про його права — це форма стандартних умов, яка на різних хмарних сервісах розташована на різних веб-сторінках, де часто містяться додаткові пояснення правовий статус яких не є зрозумілий. [12; с. 67-69]

Ще одною особливістю є те, що деякі провайдери зберігаючи дані не встановлювали можливість «пільгового» періоду для переносу своїх даних у разі припинення дії хмарного договору з тих чи інших причин чи навіть заявили, що видалення даних здійснюється виключно на їхній власний розсуд. [12; с. 70] Це становить ризик для клієнта, адже центральним елементом хмарних послуг є доступ до даних на хмарі і суворі положення щодо припинення доступу чи неможливість здійснити їх перенос на інше сховище є надто важким тягарем на нього.

Зрештою, можна загалом заперечити на всі вищенаведені ризики тим, що наразі ринок хмарний послуг характеризується тим, що не окремий постачальник хмарних послуг надає можливість укладати послуги різних видів і з різними умовами, що підлаштовує під конкретного клієнта, а навпаки серед різних постачальників хмарних послуг, кожен з яких пропонує одне чи кілька стандартизованих хмарних рішень, клієнти на практиці обирають того, який підходить до їх вимог, починаючи від умовно безоплатних, але вкрай не індивідуалізованих хмарних сервісів Google, завершуючи повністю приватними, але вартісними хмарами. [17; с. 30-31] Однак, навіть з такою позицією варто зауважити, що багато питань в договорах хмарних послуг є такими, що

вимагають певного мінімального рівня врегулювання, оскільки не всі клієнти, особливо побутові споживачі та невеликі організації, мають достатні ресурси та експертизу, щоб ретельно аналізувати та вибирати найкращі хмарні послуги для своїх потреб. Тому існує нагальна потреба у регулюванні, що встановлюватиме мінімальні стандарти для різних аспектів хмарних сервісів. Це включає такі критично важливі сфери як захист персональних даних користувачів, захист прав споживачів щодо якості послуг та інших правил для договорів про надання хмарних послуг, дотичних норми щодо прозорої хмарної та цифрової конкуренції та зрештою кібербезпеки. Саме тому ці сфери в контексті їх впливу на хмарні послуги будуть оглянуті в подальших розділах цієї роботи.

***

На основі даного розділу можна підвести такі підсумки:

1. Хмарні послуги стали невід'ємною складовою функціонування як для бізнесу, так і для персонального використання. Більшість компаній та значна частка людей використовують хмарні сервіси, в тому числі діяльність багатьох компаній є дуже залежною від них.

2. Хмарні послуги мають специфічні особливості: провайдери надають власні обчислювальні ресурси для зберігання/обробки даних користувачів, користувачі мають постійний доступ до хмари, а управління сервісами здійснюється з боку користувача здійснюється з мінімальними зусиллями. Також, існують різні моделі розподілу контролю між користувачем і провайдером, що відповідно в практиці формує різні типи хмарних послуг (IaaS, PaaS, SaaS). Водночас, можливі ситуації, коли SaaS-сервіси використовують для зберігання даних своїх користувачів сервіси PaaS/IaaS-провайдерів, утворюючи ланцюжок хмарних послуг, що ускладнює розподіл відповідальності між ними та становить інші актуальні виклики.

3. В контексті України відсутність довгий час будь-якого нормативного регулювання сприяли доктринальним дискусіям щодо правової природи договорів хмарних послуг. Однак такі в широкому сенсі вичерпуються, оскільки

більшість дослідників доходять висновку, що найбільш оптимальною договірною конструкцією є договір про надання послуг, що підтримується і публічним законодавством, який називає ці відносини як «послуги». Це накладає до договору про надання хмарних послуг деякі вимоги, такі як передбачений в ЦК України обов'язок зазначати про можливу передачу даних на зберігання до третіх провайдерів.

3. Ринок хмарних послуг характеризується домінуванням великих компаній-провайдерів, що призводить до переважної нерівності договірних відносин з клієнтами. Це зумовлює потребу у правовому регулюванні для забезпечення прозорості, хоч з іншого боку таке регулювання має бути пропорційним і уникати надмірного втручання у свободу договору.

4. Договори про надання хмарних послуг (а це в більшості випадків типові договори, які можна тільки прийняти без змін) часто надають більше прав провайдерам, звужують права користувачів і не завжди належно покривають ризики для останніх.

5. Також, актуальною є проблема успадкування даних на хмарних сервісах. Договори між хмарними провайдерами та фізичними особами зазвичай не регулюють це питання успадкування або не здійснюють це достатньо гнучко. Водночас, врегулювання питання успадкування даних у хмарних сервісах вимагає ретельного аналізу та балансування інтересів спадкоємців, волі померлого власника даних та можливостей хмарних провайдерів запровадити відповідні процедури.

6. Актуальним питанням є фрагментація даних хмарними провайдерами, що часто застосовується з технічних міркувань і несе ризики щодо відповідності нормам щодо захисту даних, адже передбачає часто слабоконтрольовані транскордонні передачі даних.

7. Актуальною проблемою є те, що стандартні умови хмарних сервісів часто складно сформульовані, а користувачі рідко їх читають в поєднанні з тим фактом, що форма подачі умов ускладнює розуміння їх правового статусу. Втім багато з цих умов містять критично важливі положення для споживачів, зокрема

ті що ознайомлюють з можливістю втрати доступу до даних при припиненні договору, а також відсутності пільгового періоду для перенесення.

8. Попри варіативність хмарного ринку і наявність різного роду рішень від різних провайдерів, все ж існує потреба у базовому регулюванні з мінімальними стандартами захисту прав споживачів, персональних даних, конкуренції, кібербезпеки, що спрямована переважно на захист споживачів та невеликих організацій як клієнтів хмарних послуг.

РОЗДІЛ 2.
ТЕНДЕНЦІЇ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА БЕЗПЕКИ ДАНИХ ПРИ НАДАННІ ХМАРНИХ ПОСЛУГ

2.1. Тенденції правового регулювання захисту персональних даних користувачів хмарних послуг

В загальному, на рівні Європейського Союзу відсутнє спеціальне законодавство, яке регулює хмарні послуги. Відтак правове регулювання стосовно таких застосовується в рамках різних сфер регулювання, які в певній мірі стосуються хмарних послуг. Однією з таких сфер є захист персональних даних, яка загалом в Європейському Союзі є гарно врегульована.

Однак в продовження ідеї про те, що не існує окремого регулювання щодо правових відносин захисту персональних даних в хмарі, існує думка, що хмарні послуги не становлять нові чи унікальні виклики для сфери законодавства про захист прав споживачів. [20; с. 118] Водночас, частково погоджуючись з нею, зауважу, що низка особливостей хмарних послуг, що вирізняють їх з-поміж інших цифрових послуг, є достатньою підставою розглядати певні складнощі в забезпеченні приватності, які виникають через особливості хмари як такої, що зумовлює потребу здійснювати їх дослідження.

Центральним актом цієї сфери є загальний регламент про захист даних (GDPR), що був прийнятий Європейським Союзом і почав діяти в 2018 році та вважається найсуворішим актом щодо захисту персональних даних у світі.[18] Його істотною рисою є екстериторіальність, тобто ознака, яка з певними винятками розповсюджує норми про захист персональних даних на суб'єктів поза межами Європейського Союзу, якщо вони пропонують свої послуги суб'єктам персональних даних в ЄС чи здійснюють моніторинг їх поведінки. [19] Загалом саме ця риса робить положення GDPR важливими також і для хмарних

провайдерів, які розташовані у США (як-от Amazon, Google та Microsoft) та в інших країнах і змінює стандарти їх діяльності глобально, що безпосередньо впливає за умови хмарних послуг, що надаються на ринку всього світу.

Характеристику GDPR слід почати з того, що його регулювання стосується тільки персональних даних, тобто тих даних за якими можна ідентифікувати особу. [22, ст. 4(1)] Однак як випливає з природи хмар, а саме таких характеристик, оглянутих в першому розділі, як надання безперервного і постійного доступу на вимогу та мінімізація управлінських зусиль, надавач хмарних послуг не може (а й інколи ніколи такого не робить) весь час контролювати дані, які надаються клієнтом, в тому числі на предмет наявності серед цих даних персональних. На мій погляд і як показує практика, що буде описана надалі, це означає, що хмарні провайдери, не знаючи, чи є персональні дані у тому обсязі даних, що надсилає на їх хмару клієнт, повинні презюмувати позитивну відповідь на це твердження. Це, на мою думку, призводить до того, що практично всі хмари будуть підпадати під дію GDPR і не знаючи, які конкретні дані вони обробляють, застосовувати вимоги цього регламенту до всіх даних клієнтів.

Також, GDPR характеризується тим, що передбачає ряд принципів. До них входять принципи законної, справедливої та прозорої обробки, принцип визначених, чітких і законних цілей збирання та обробки даних, принцип мінімізації даних, точності даних, обмеження зберігання даних та зрештою принцип цілісності і конфіденційності. [21] Однак навіть в реалізації деяких з цих принципів щодо хмар є певні особливості.

Розглядаючи принцип прозорості, варто зауважити, що він зокрема полягає в забезпеченні наступного:

«…що контролери даних повинні представляти інформацію/комунікацію ефективно та стисло, щоб уникнути інформаційної втоми. Ця інформація повинна бути чітко відокремлена від іншої інформації, що не стосується приватного життя, наприклад, договірних положень або загальних умов використання. В онлайн-контексті використання багаторівневої заяви/повідомлення про конфіденційність дозволить суб'єкту даних перейти до конкретного

розділу заяви/повідомлення про конфіденційність, до якого він хоче отримати негайний доступ, замість того, щоб прокручувати великі обсяги тексту в пошуках певних питань.» [23; с. 7]

Це може передбачати використання окремих політик приватності на сайті, однак через хмарні технології виконання умов щодо прозорості в певних аспектах може бути ускладнено. Зокрема, це стосується описаної особливості щодо складності відносин хмарних послуг, де різні хмари можуть бути клієнтами один одного і зберігати інформацію кінцевого клієнта через розшарування хмар, що зазначалося в попередньому розділі, і що призводить до того, що хмарний провайдер в дотримання принципу прозорості має розкривати тих провайдерів, яким він передає дані. Однак, як вказують дослідники, ці ланцюжки хмарних зв'язків між провайдерами є надто складними, аби їх повний зміст підпадав під вимогу «ефективного і стислого повідомлення, яке уникає інформаційної втоми». [24; с. 16-18] На практиці хмарні сервіси як-от Google Cloud розкривають цю інформацію шляхом надання списку інших хмарних сервісів, яким вони передають дані. [25]

На підставі зазначеного можна підійти до висновку, що часто технічні та організаційні особливості хмарних послуг є надто складні для розуміння звичайних користувачів, як суб'єктів персональних даних, водночас принцип прозорості змушує надавачів хмарних послуг надавати інформацію пов'язану з персональними даними такими способами (а відповідно спрощувати), аби вона була достатньо доступна суб'єкту і викладена стисло. Це в свою чергу змушує хмари орієнтуватися на ці вимоги при розроблені публічно доступних політик.

Також, важливою ознакою GDPR є наявність прав суб'єктів даних, реалізація і дотримання яких зобов'язує також і хмарні сервіси. [27; ст. 12-22] Серед цих прав досить актуальним для хмарних сервісів те, яке передбачено статтею 20 GDPR — право на мобільність даних. Воно включає 2 основні обов'язки з точки зору надавача хмарних послуг, що здійснюється на вимогу суб'єкта даних: (i) обов'язок надавати у загальновживаному та машиночитаному форматі та без перешкод суб'єкту дані, що його стосуються та (ii) обов'язок

прямої передачі даних іншому контролеру (на практиці – іншому хмарному провайдеру), якщо це технічно можливо. [28]

Дослідники вказують що обов’язок прямої передачі часто не є технічно можливим між двома різними хмарними провайдерами, що відповідно обмежує застосування другого обов’язку. [24; с. 37-39] Попри це інші дослідження показують, що серед користувачів є надзвичайно великий попит на полегшену мобільність даних. [29] Таким чином, постає необхідність в розробці політики, яка дозволить полегшувати реалізацію можливості мобільності даних між різними хмарними платформами для задоволення потреб користувачів та дотримання вимог GDPR. З іншого боку, питання забезпечення належної мобільності даних стосується не тільки сфери захисту персональних даних, а й політик ЄС в інших сферах, де спостерігаються активні дії щодо розвитку цього питання, що буде детальніше розглянуто в третьому розділі.

Центральним елементом для розуміння того, як GDPR застосовується до провайдерів хмарних послуг і які конкретні обов’язки на них покладаються, є поняття "контролер" та "процесор" персональних даних, які визначаються в цьому Регламенті. Контролером є суб'єкт, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних. Процесор же — це суб'єкт, який лише здійснює обробку даних за дорученням контролера. [22; ст. 4(7-8)] Сутність такого розмежування полягає в тому, що GDPR покладає основну відповідальність за дотримання принципів поводження з персональними даними на контролера, навіть якщо він передав дані на обробку процесору. Втім, деякі зобов'язання, такі як забезпечення належних технічних і організаційних заходів безпеки, покладаються Регламентом безпосередньо і на процесора даних. [30]

У своїй діяльності хмарні провайдери можуть виконувати різні ролі щодо персональних даних - як контролерів, так і процесорів. Коли хмарний сервіс лише надає місце для зберігання даних клієнтам і не здійснює жодних операцій з цими даними, не маючи навіть інформації про наявність у них персональних даних, то в такому випадку провайдер виступає процесором. Однак, стосовно даних, що провайдер самостійно застосовує у своїй діяльності (наприклад,

електронні адреси, номери телефонів чи імена при реєстрації користувачів — тобто метаданих), він діє як контролер персональних даних. Деякі провайдери (як-от Facebook), що пропонують послуги моделі "програмне забезпечення як сервіс" (SaaS), прямо зазначають, що розглядають себе виключно як контролерів даних користувачів. [31; с. 10-12] Така ситуація може пояснюватися тим, що такі сервіси здійснюють завжди первинно обробляють всіх дані від клієнта, зокрема, для маркетингових цілей.

Як випливає з вищеописаного явища розшарування хмар, провайдери передають свої дані іншим провайдерам для звичайних цілей зберігання. В такому випадку первинний провайдер (наприклад, Facebook, який отримав дані від користувача в додатку) виступає контролером відносно даних суб'єкта даних, а той, якому він передав (як-от AWS, сервера якого Facebook використав б як сховище для даних про користувачів) – процесором.

У зазначених випадках, відповідно до вимог GDPR має укладатися договір, в якому встановлюється предмет і тривалість обробки , характер і мета обробки, тип персональних даних і категорії суб'єктів даних, а також обов'язки та права контролера, а також низка інших вимог. [27; ст. 28(3)]

Загалом, оскільки процесор несе велику частину відповідальності щодо захисту персональних даних суб'єкта, то він зацікавлений в суворих умовах подібного контракту, які зокрема, забезпечать йому можливість здійснювати запити суб'єкта на реалізацію своїх прав тощо. Окрім того, частина 1 статті 28 Регламенту зобов'язує контролера використовувати лише тих процесорів, які надають достатні гарантії для впровадження відповідних технічних та організаційних заходів безпеки. [27; ст. 28(1)]

Таким чином, для сторони контролера (наприклад, компанії чи організації, що обробляють дані суб'єктів персональних даних) вибір хмарного провайдера, який повністю відповідає вимогам GDPR та відповідним стандартам, є вкрай важливим. З іншого боку, це зумовлює хмарних провайдерів не лише надавати сервіси хмарних послуг, але й гарантувати дотримання вимог щодо захисту прав персональних даних. Цей додатковий сервіс фахівці називають "комплаєнс як

послуга". [32; с. 1, 3-6] Зокрема, такий сервіс вже повністю використовується багатьма хмарними платформами як-от Google Cloud. [33] Інституції Європейського Союзу підтримують таку тенденцію і сприяють таким політикам як EU’s Cloud Code of Conduct. Згідно з цим кодексом, Європейська рада з захисту даних затвердила чіткі критерії, за якими хмарні провайдери забезпечують відповідність вимогам GDPR. Крім того, передбачено створення моніторингової організації, яка має здатність робити висновки та надавати рекомендації з питань комплаєнсу таких компаній, що дає змогу клієнтам хмарних послуг, які є контролерами персональних даних бути впевненим у можливості передавати дані тим чи іншим хмарним провайдерам як процесорам. [34]

Таким чином, хоча хмарні провайдери традиційно мають сильну ринкову і переговірну позицію і навряд чи змінювали б свої типові договори за вказівкою окремих бізнесів задля посилення захисту персональних даних, GDPR як регулювання зробило обов'язок клієнтів хмар як контролерів даних щодо належного вибору процесорів рушійною силою, яка змусила хмарні сервіси адаптувати свої послуги і контракти відповідно до вимог захисту персональних даних.

Однак, хмари можуть виступати не тільки просто процесорами чи контролерами персональних даних. Вони також можуть підпадати також під одну з похідних ролей — бути спільними контролерами або субпроцесорами, кожна з яких має свої особливості.

Ідея спільних контролерів проста у своїй суті — це декілька суб’єктів, які разом (тобто без нерозривно пов’язано) виконують роль контролера певних персональних даних (тобто, за визначенням, спільно встановлюють цілі та засоби обробки таких). [27; ст. 26] Але на практиці це стає складнішим, оскільки в ускладнених системах обробки даних і відносинах між сторонами може виникнути спільний контроль даних, навіть якщо він не передбачений договором між цими сторонами (наприклад здійснюватися фактично, що потім може бути визнано судом). [39; с. 12-13]

Наприклад, справа Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV у Суді Європейського Союзу (відома як справа Fashion ID) стала важливою, оскільки в її рішенні було встановлено, що інтернет-магазин, який встановив плагін Facebook, є спільним контролером даних з Facebook, і було зроблено висновок, що цілі та методи обробки даних визначаються спільно, незважаючи на те, що інтернет-магазин не мав доступу до даних, які передавалися через плагін Facebook. [39; с. 16-18]

Інше рішення, яке підкреслює широкий підхід до тлумачення спільного контролю, є рішення Суду ЄС, відоме як Wirtschaftsakademie, де було визнано, що сторінка у Facebook, яка отримувала статистику про користувачів сторінки через внутрішній інструмент Facebook є спільним контролером персональних даних з ним . Однак, з іншої сторони, як і в попередній справі, Суд наголосив на різній ступені відповідальності Facebook та сторінки-користувача його інструментом як спільних контролерів, адже вони мали різний ступінь впливу на дані. [39; с. 14-15]

Однак на думку деяких дослідників, Суд Європейського Союзу, намагаючись забезпечити повний і ефективний захист даних суб'єктів, розширив концепцію "спільного контролера" до такої міри, що це може підірвати важливий зв'язок між відповідальністю та фактичним контролем над обробкою персональних даних. [35] Я погоджуюся з такими висновками, і хочу зазначити що широка інтерпретація поняття спільного контролера може призвести до ситуацій, коли вони не розуміють до кінця своїх обов'язків і відповідальності, що може зашкодити прозорості обробки даних для суб'єктів даних. Така розмитість і невизначеність замість посилення захисту може фактично послабити ефективний захист персональних даних.

Однак в будь-якому випадку, можна підійти до висновку, що тлумачення ролі хмарного провайдера не є повністю визначеним (в тому числі договором), а має ретельно оцінюватися фактично самим провайдером, і сторонами, які передають дані таким провайдерам у кожному окремому випадку, зокрема для того, аби чітко розуміти свої права та обов’язки та інформувати суб’єктів про

залучення третіх сторін в тій чи іншій ролі (в тому числі, в межах описаного принципу прозорості).

Також, як було зазначено, хмарні провайдери також можуть виступати в ролі субпроцесорів. Субпроцесор — це особа, якій передає дані процесор і яка діє згідно з інструкціями процесора. Варто зазначити, що субпроцесор може бути залучений лише за умови письмового дозволу від контролера даних або спільних контролерів. У такому випадку процесор повинен укласти із субпроцесором обов'язковий договір, який детально визначає відповідальність субпроцесора. Цей договір має забезпечувати такий самий рівень захисту персональних даних, як і первинний договір між контролером і процесором. [36]

Загалом, дослідники зазначають, що такі суворі вимоги щодо залучення субпроцесора зумовлені тим, що практика орієнтована на те, щоб контролери даних зберігали контроль над персональними даними в усьому ланцюжку процесорів і субпроцесорів, адже саме контролери відповідальні за дотримання більшості вимог щодо захисту персональних даних. [37] Однак, на мій погляд, з огляду на вищеописану тенденцію розвитку практики комплаєнс як послуги, вибір належних субпроцесорів організаційно є часто завдання хмарних провайдерів як процесорів і здійснюється без активної участі чи згоди контролерів.

Такий перерозподіл відповідальності може здаватися прийнятним і зручним для низки організацій як контролерів, адже забирають в них тягар здійснювати пошук прийнятних субпроцесорів, ознайомлюватися з ними та перевіряти їх на відповідність. Однак для інших така практика може істотно порушувати їх інтереси. Зокрема, Європейський інспектор із захисту даних під час розслідування використання інституціями ЄС продуктів і послуг Microsoft у 2020 році визнав умову щодо права органів ЄС як контролерів заперечувати про залучення нового субпроцесора тільки шляхом розірвання договору про надання хмарних послуг, такою що надає замало вибору органам ЄС, які не погоджуються з призначенням нового субпроцесора, і створює відповідні ризики. Таким чином, було зроблено висновок, що контролер, який передає

масштабні обробки, повинен мати "значущу" процедуру схвалення субпроцесорів. [38; п. 72-75]

Ще однією з ключових особливостей, що свідчить про суворий підхід GDPR, є його унормування транскордонної передачі персональних даних до третіх країн, які не входять до складу Європейського економічного простору. Дані обмеження застосовуються як до передачі даних між контрагентами, так і до внутрішньокорпоративного обміну даними між підрозділами однієї організації, розташованими в різних юрисдикціях. [39]

За загальним правилом, GDPR встановлює заборону на передачу персональних даних до третіх країн, які не забезпечують належного рівня захисту. Для того щоб цей належний рівень захисту гарантувати сторони повинні покладатися на один із дозволених механізмів передачі даних, таких як рішення про адекватність, стандартні договірні положення (SCC), обов'язкові корпоративні правила (BCR), відсупи для спеціальних ситуацій тощо. [40; с. 30, 46]

Рішення Європейської Комісії про адекватність приймається щодо законодавства певної третьої країни у сфері захисту персональних даних, рівень захисту якої визнається не слабшим за рівень захисту в ЄС. За наявності такого рішення дані можуть вільно передаватися до цієї юрисдикції. [40; с. 30, 46]

Другим механізмом є гарантії відповідності вимогам GDPR, що включають стандартні договірні умови (SCC) та обов'язкові корпоративні правила (BCR). SCC встановлюють договірні зобов'язання сторін щодо захисту даних при їх трансфері, а також передбачають постійний моніторинг ризиків. BCR діють в рамках однієї компанії чи групи й запроваджують внутрішні правила захисту даних при передачі за межі ЄС. [40; с. 34, 42]

Останнім механізмом є відступи для конкретних ситуацій передачі даних, проте їх застосування є досить обмеженим, особливо для надання масштабних транскордонних послуг як-от хмарні. [40; с. 52-55] Відтак варто сконцентруватися на особливостях застосування та тенденціях розвитку перших двох механізмів передачі в контексті хмарних послуг.

Характеризуючи особливість рішень про адекватність варто згадати знакову історію становлення такого рішення відносно США, яка в контексті хмарних послуг є особливо актуальною, адже як було вказано низка найбільших провайдера хмарних послуг на світовому ринку засновані в США.

Передача персональних даних між ЄС та США протягом останніх двох десятиліть характеризується складними законодавчими та судовими випробуваннями. Первинно режим передачі даних між США та ЄС було встановлено у 2000 році, коли було запроваджено механізм "US Safe Harbor", що уможливлював передачу даних до США для компаній, які дотримувалися встановлених принципів конфіденційності. Проте у 2015 році Суд Європейського Союзу анулював чинність цієї угоди (рішення у справі Schrems I), аргументуючи порушенням прав громадян ЄС на приватність через можливий доступ американських спецслужб до цих даних. Спроба відновити систему передачі даних між двома регіонами була здійснена у 2016 році шляхом укладення угоди "EU-US Privacy Shield". Втім, у 2020 році Суд ЄС знову визнав цей механізм недійсним у справі Schrems II через недостатність захисту рівня захисту, знову ж через проблему недостатньо контрольованого урядового доступу. За відсутності чинного механізму передачі даних до США компанії змушені були вдаватися до альтернативних методів, як-от стандартні договірні положення. Однак ці методи є менш оптимальними та теж юридично вразливими до оскарження прихильниками конфіденційності, що враховуючи масовість передачі даних між ЄС та США, зокрема хмарними сервісами, є надто обтяжуючим з практичної точки зору. [41] Тому, 10 липня 2023 року в рамках спеціальної угоди «EU-US Data Privacy Framework» прийнято рішення про адекватність юрисдикції США, однак накладено певні вимоги до діяльності органів спецслужб США стосовно персональних даних, надано право особам з ЄС мати доступ до незалежного та неупередженого механізму правового захисту щодо збору та використання їхніх даних такими службами США, який включає створений суд із захисту даних (DPRC) та запроваджено деякі інші гарантії. [42] Однак на думку аналітиків, навіть таке рішення буде оспорюватися в Суді ЄС і є

достатні підстави очікувати так-званий Schrems III, тобто рішення, яке вкотре визнає недостатньою і цю угоду щодо забезпечення рівня відповідності в межах рішення про адекватність. [43]

В межах подібної практики можна зробити висновок, що норми Європейського Союзу щодо захисту персональних даних, зокрема вимоги до передачі даних за кордон, справляють істотний вплив на світове регулювання в цій сфері. Незважаючи на певний спротив, наявність інституту адекватного рівня захисту даних при їх передачі до третіх країн, таких як США, стимулюють зміни в законодавстві та практиках цих держав на користь вимог щодо рівня захисту персональних даних, які рівняються на досвід, що встановлений GDPR. Це в свою чергу, враховуючи обсяги глобальної передачі даних через хмари, змушує компанії адаптувати свої політики конфіденційності та процедури обробки даних до жорстких європейських стандартів.

Характеризуючи другий механізм передачі персональних даних в треті країни, гарантії відповідності вимогам GDPR, що включають стандартні договірні умови (SCC) та обов'язкові корпоративні правила (BCR), варто зауважити, що застосування таких в контексті хмарних послуг становить певні практично-правові складнощі.

Це обумовлюється тим, що оскільки SCC та BCR є загалом механізмами, що застосовуються при відсутності такого механізму як рішення про адекватність, тобто передбачається, що загальний рівень захисту персональних даних у таких юрисдикціях є нижчим ніж у ЄС, тому для його підвищення потрібно включити додаткові договірні чи внутрішньо-корпоративні зобов’язання. Водночас, як зазначається дослідниками, додаткові технічні чи організаційні заходи, можуть бути недостатніми для цієї мети, особливо, що стосується взаємодії отримувача з наданням доступу до даних на вимогу органів влади. Навіть якщо імпортер даних фактично не є об'єктом таких вимог, сама наявність відповідних повноважень, вже створює ризики для даних, які складно подолати договірними умовами. [40; с. 40-44]

Тому, пошук ефективних та реалістичних рішень для безперешкодного транскордонного обміну даними в рамках хмарних сервісів залишається вкрай складним питанням як в контексті практики застосування регулювання, що може мати труднощі у вирішенні навіть через такі індивідуалізовані механізми як стандартні договірні умови (SCC) чи обов'язкові корпоративні правила (BCR).

Центральним актом, що регулює захист персональних даних в Україні є Закон України «Про захист персональних даних» (далі тут – Закон). [92] Загалом в деяких цей закон є подібний до GDPR, тому подальший аналіз в контексті хмарних послуг доцільно здійснювати в порівнянні з цим регламентом. Як і GDPR, Закон захищає виключно відомості про фізичну особу за якими вона може бути ідентифікована. [92; ст. 2] Однак, як зазначалося вище з технічно-організаційних причин хмара не може в кожному випадку визначати чи обробляє користувач саме персональні дані чи ні, тому їх обробка як правило презюмується для цілей хмарної обробки.

Іншим аспектом є роль хмари в обробці персональних даних. В законі виділяються дві ключові ролі: (i) володілець персональних даних як фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом; та (ii) розпорядник персональних даних як фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця. [92; ст. 2] Ці суб'єкти є функціонально подібними до відповідно контролера і процесора за GDPR і як було вказано, хмарні провайдери залежно від конкретної ситуації і конкретних функції можуть виконувати і тим і тим агентом відносно персональних даних, а також поєднувати ці ролі. Однак, на відміну від GDPR Закон не має аналогів щодо субпроцесора та спільного контролера. І якщо, як зазначалося, функція спільного контролера піддається сумнівам з боку дослідників, то субпроцесори є надзвичайно поширеними суб’єктами в практиці хмарних послуг через наявність усталеної практики розшарування хмарних сервісів з утворення ланцюжку. Водночас Закон не передбачає подібних суб’єктів і дані від розпорядників можуть передаватися

лиш третім особам. Однак зі зобов’язань третіх осіб існує лиш те, що доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог цього Закону або неспроможна їх забезпечити. [92; ст. 16(2)] Однак цього надто мало для того аби володілець даних міг мати достатньо контролю щодо такої третьої особи, зокрема не вказано договірний спосіб зобов’язань, обмеження обсягу і гарантій щодо обробки даних тощо.

Актуальним питанням є ефективність практики застосування положень цього Закону для захисту персональних даних. Деякі дослідники, такі як Е. Р. Євлахова стверджують, що

«…в Україні успішно функціонує інститут захист прав та інтересів суб’єктів персональних даних, зокрема і користувачів хмарних послуг, що надають свої персональні дані надавачам хмарних послуг для їх подальшої обробки». [93; с. 39]

Свою думку дослідниця підкріплює однією зі справ судової практики з успішним притягнення до адміністративної відповідальності.

Втім я категорично не можу погодитися з цією думкою, підкріплюючи це наступними аргументами:

По-перше, якщо взяти загалом практику успішного накладення штрафу за 188-39 КУпАП (тобто за порушення в сфері персональних даних), то таких випадків за останні 5 років лише близько 40 і суд майже завжди накладає мінімальний штраф (5100 грн для суб’єктів господарської діяльності).[1] [94; ст 188-39]

По-друге, аналізуючи вказану статтю КУпАП, варто зазначити, що максимальний штраф навіть за повторне порушення, який передбачається це 2000 неоподатковуваних мінімумів, що враховуючи великі розміри хмарних провайдерів (що описувалося в першому розділі) є неспівмірним для ефективних санкцій щодо їх порушень з персональними даними, які можуть становити загрозу для сотень тисяч осіб. [94; ст 188-39] Для порівняння штрафи за GDPR

[1] Пошук через ресурс Verdictum.ligazakon за статтею 189-39 КУпАП: https://verdictum.ligazakon.net/result?group_filter=5&stored_extr_status_code_filter=50&p=1&c=30&links_npa=KD0005%20984414

можуть досягати 20000000 євро або, у випадку підприємства, до 4 % від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою. [27; ст. 83(6)]

По-третє, цивільно-правовий спосіб захисту теж не можна вважати ефективним. Як зазначають оглядачі судової практики, суди досить обмежено стягують морально шкоду за порушення персональних даних, а їх практика не достатньо послідовного тлумачення норм щодо порушення персональних даних є досить несприятлива для ефективного захист своїх прав. [95]

По-четверте, в Україні відсутній окремий орган, який здійснює контроль у сфері захисту персональних даних, а цю функцію покладено на Уповноваженого Верховної Ради України з прав людини, що дає можливість стверджувати про обмежені ресурси для забезпечення виконання регулювання у цій сфері. [92; ст. 23(1)]

Отже, можна стверджувати, що українське законодавство в сфері захисту персональних даних і його практика застосування є такими, що мають потенціал для подальшого розвитку. Говорячи про цю тенденцію, варто звернути увагу на законопроекти, які загалом напрямлені на усунення вказаних вище недоліків: проект Закону «Про захист персональних даних» №8153 від 25.10.2022 та проект Закону «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» № 6177 від 18.10.2021. [96] [97]

Ці проекти передбачають глобальне покращення законодавства і вводять зокрема такі актуальні для хмарних послуг положення як: (i) збільшення штрафів до 150 мільйонів гривень або до 8% загального річного обороту юридичної особи, що робить санкції ефективними навіть щодо найбільших хмарних компаній, що домінують на ринку; (ii) окремий орган з питань захисту персональних даних з чітко визначеними широкими повноваженнями та з окремою службою інспекторів для здійснення перевірок та (iii) появу низки визначень і деталізацій процедур, що збільшує правову визначеність як-от вимоги до залучення оператором (аналог процесора в GDPR) іншого оператора (аналог субпроцесора) тощо. [96; ст. 31, 32, 59] [97; ст. 15, 45]

Отже, можна підсумувати, що основною тенденцією в сфері захисту персональних даних в Україні є наближення до європейського законодавства, яке передбачає набагато більш ефективне регулювання і правозастосування, зокрема шляхом глобальної зміни регулювання цієї сфери шляхом очікуваного прийняття законопроектів №8153 та № 6177. В контексті хмарних послуг це матиме наслідком появу більш ефективних і визначених норм, які регулюватимуть діяльність хмарних провайдерів та дійсно впливатимуть на них, заохочуючи розвивати найкращі практики із захисту персональних даних.

2.2. Тенденції правового регулювання безпеки даних в хмарах

Як зазначалося, одним із принципів обробки даних за GDPR є цілісність та конфіденційність. Вони передбачають, що дані мають обробляються у спосіб, що забезпечує належну безпеку персональних даних, включаючи захист від несанкціонованої або незаконної обробки, а також від випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів. [27; ст. 5(1)(f)] Стаття 32 GDPR уточнює ці вимоги і зобов'язує зважаючи на сучасний рівень розвитку, витрати на реалізацію, специфіку, обсяги, контекст і цілі опрацювання, а також ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, які викликає опрацювання, контролера і оператора вжити необхідних технічних і організаційних заходів для забезпечення рівня безпеки відповідно до ризику. [27; ст. 32]

Втім такі засоби кібербезпеки не регулюються виключно GDPR, а також включаються в сферу дію спеціальних законів, що спрямовані на захист інформаційної безпеки. Перший з таких, так Директиві (ЄС) 2015/1535 (відома як директива NIS) визначила надавачів хмарних послуг як постачальники цифрових послуг (DSP) і наклала на таких постачальників вживати заходи щодо зокрема безпеки систем і засобів, розгляду інцидентів, управління безперервністю бізнесу, моніторинг, аудит, тестування і відповідності

міжнародним стандартам. Однак ця директива була замінена Директивою (ЄС) 2022/2555 (відома як директива NIS 2), яка в порівнянні з першою посилює і розширює сферу своєї дії, норми якої будуть застосовні з жовтня 2024 року. [44] Центральним елементом цієї директиви, є поділ суб'єктів, які підпадають під дію Директиви на основних (essential) і важливих (important). Надавачі хмарних послуг поряд з надавачами послуг енергетики, питної води, залізничного транспорту, охорони здоров'я тощо відносяться до основних суб'єктів, що підлягають більш суворішому рівню регулювання. [45] Це правило застосовується з певними винятками, якщо надавач хмарних послуг має менше 250 співробітників або оборот до 50 мільйонів євро, однак в межах аналізу ринку у першому розділі, можна зробити висновок, що такий розмір не є притаманний ринку хмарних послуг. [46]

До хмарних провайдерів як основних суб'єктів буде застосовуватися вимоги оцінки ризиків і політики безпеки для інформаційних систем, політики та процедури використання криптографії та, у відповідних випадках, шифрування, процедури безпеки для співробітників та низка інших. [47] Також, на відміну від важливих суб'єктів, до хмарних послуг як основних будуть вживатися низка заходів *ex ante*, таких як вимога систематичного документування відповідності заходам з управління ризиками кібербезпеки, регулярні фактичні перевірки, цільові аудити безпеки тощо. [48; п. 122, 124]

Втім деякі дослідники підходять критично до ініціативи NIS2, вважаючи що настільки широкий контроль над хмарними провайдерами може призвести до ситуації, коли наглядовим органам не вистачатиме ресурсів для такого обсягу контролю. На їх думку, краще зосередитися лише на найбільш критичних хмарних сервісах, застосовуючи до них превентивний (*ex ante*) нагляд, а до решти - лише реактивний (*ex post*) контроль після інцидентів. Такий підхід пропонує, зокрема, уряд Великобританії у своїх поправках до національного законодавства після виходу з ЄС. Це дозволить регуляторам ефективніше використовувати обмежені ресурси, фокусуючись на найбільш ризикованих сервісах. [49; с. 45-46]

Загалом, можна зробити висновок, що Директива NIS 2 відносячи хмарних провайдерів до категорії "основних суб'єктів" нарівні з такою критичною інфраструктурою як енергетика, транспорт, охорона здоров’я, вказує про серйозність намірів правової політики ЄС в питаннях регулювання захисту інформації хмарними провайдерами, що на мій погляд, пов’язується з дедалі важливішою роллю інформації у суспільстві, а також з тим, що хмарні сховища дуже часто оперують надзвичайно важливими, чутливими даними, на операції з якими покладаються численні компанії, організації, уряди й багато людей, а втрата чи витік цих даних в наш час може спричинити надто істотні наслідки для бізнесу, держав, конфіденційності громадян. Попри те, що можуть існувати певні практичні складнощі в реалізації (зокрема, через обмеженість ресурсів наглядових органів) і від того подальші калібрування в масштабах застосування нагляду, подібні ініціативи чітко окреслюють тенденцію правого регулювання в тому, щоб підсилювати вимоги і здійснювати контроль над їх виконанням щодо аспекту кібербезпеки і захисту даних при наданні хмарних послуг.

Говорячи про українські тенденції правового регулювання безпеки даних у хмарах, варто згадати закон України «Про хмарні послуги», який встановлює загальні засади регулювання цієї сфери, переважно що стосується даних, якими оперують публічні розпорядники. [83]

Відтак, основною особливістю закону є те, що він характеризується диференційованим підходом залежно від суб'єктного складу правовідносин. Зокрема, він приділяє підвищену увагу регламентації договірних відносин щодо послуг хмарних обчислень та/або центрів обробки даних, у випадках коли стороною договору виступає публічний орган та/або критично важливий об’єктам інфраструктури. Натомість, правове регулювання набуває більш обмеженого характеру у ситуаціях, коли учасниками таких договірних правовідносин є виключно приватні суб'єкти господарювання. [84]

Зокрема договір хмарних послуг з публічними чи суб’єктами критичної інфраструктури має базуватися на основі типового договору, затвердженого КМУ, і включати положення про вимоги щодо негайного оповіщення про

інциденти кібербезпеки, вимоги до безперебійності роботи системи, порядок та строки передачі даних і систем між сторонами, порядок припинення договору, включаючи строки та процедури передачі даних і систем тощо. [83; ст. 10(3)] Окрім цього, передбачається що до договору має застосовуватися право України, а справа у разі спору бути підсудна судам України, а також обов'язок здійснювати пошук хмарного провайдера відповідно до законодавства про публічні закупівлі. [83; ст. 10(3), ст. 11(2)] Водночас, до хмарних відносин між приватними суб'єктами подібних вимог немає.

Загалом на основі висновків дослідників закону можна зазначити, що Закон «Про хмарні послуги» є досить рамковим, і багато в чому реалізація державної хмарної політики залежатиме від того, наскільки буде ефективна діяльність регулятора (наразі це Адміністрація Державної служби спеціального зв'язку та захисту інформації України) та прийнятих підзаконних актів на виконання цього закону. [85; с. 84-85]

Іншим суттєвим викликом для державної хмарної політики в контексті безпеки даних є російське вторгнення в Україну з 2022 року. Оскільки, роль даних в суспільстві і в тому числі у державних процесах є критичною, а воєнні дії є прямою небезпекою для хмарних серверів, де зберігаються публічні дані, бази даних реєстрів, службові дані органів влади тощо, то постало питання збереження таких у воєнних умовах. Це все відбувалося на фоні недостатньої матеріальної та організаційної бази щодо збереження подібних даних, зокрема на початок вторгнення деякі з таких даних, ймовірно, навіть не мали резервного копіювання. [86]

Відтак, такі обставини зумовили прийняття рішень на можливість обробки даних у закордонних хмарах. Так 8 березня 2022 року Національним банком було прийняте рішення, що дозволяє протягом воєнного стану та протягом двох років після його скасування зберігати дані клієнтів та інформацію, що містить банківську таємницю у хмарних сервісах, що надаються з використанням обладнання, яке розташовано в державах – учасницях ЄС, Європейського співтовариства, Великій Британії, США або Канаді. [87] Окрім цього, 4 серпня

2022 року Національна комісія з цінних паперів та фондового ринку дозволила використання хмарних сервісів розташованих в країнах, що є членами ЄС, у Великої Британії, США, Канаді для, зокрема, Центрального депозитарію та депозитарних установ. Також, 30 грудня 2022 року Кабінет Міністрів України прийняв рішення, яке дозволяє після погодження Службою Безпеки України передачу державних інформаційних ресурсів (публічних електронних реєстрів), які не містять службової інформації та інформації, що становить державну таємницю, та їх резервних копій розміщати на хмарах, що розташовані за межами України, за умови виконання певних вимог (як-от криптографічного захисту) та процедур. [88] Зрештою, змінами до закону «Про хмарні послуги» від 16.01.2024 встановлено навіть, що за деяких умов під час дії воєнного стану розміщення даних, що містять державну таємницю, Міністерства оборони України, Збройних Сил України та військових формувань, може здійснюватися на території держав-членів НАТО із застосуванням хмарних ресурсів, якщо було досягнуто спільного рішення Міністра оборони України та Генерального штабу Збройних Сил України з невідкладним повідомленням відповідного комітету Верховної Ради України. [89]

Також в межах приватних організацій спостерігається тенденція до зміни власних хмарних стратегій у відповідь на виклики війни. Так, компанія EasyPay, для якої безперебійність роботи є критичною, створила повністю ізольовану приватну хмару, налаштовану під свої потреби. Це дозволило розподілити основні дані та сервіси між власним дата-центром та приватною хмарною інфраструктурою, підвищивши відмовостійкість IT-системи в умовах воєнного часу. [90]

Отже, у зв'язку з російським вторгненням в Україну виникли нові тенденції розвитку ринку хмарних послуг. Воєнні дії безпосередньо загрожують фізичній цілісності серверів, на яких розміщуються критично важливі дані державних органів та реєстрів, також це стосується і хмар багатьох бізнес-користувачів з приватного сектору. Це зумовило необхідність пошуку комплексних рішень щодо локалізації даних та забезпечення їх безпеки. Державна політика

опинилася перед складним вибором: з одного боку, потреба у збереженні хмарного суверенітету щодо державних інформаційних ресурсів, а з іншого – необхідність розміщення даних поза межами країни для підвищення їх фізичної безпеки. Загалом, регулятори дозволили за певних умов передавати ряд державних інформаційних ресурсів на хмарні сервіси, розташовані на території країн-членів НАТО та інших країн, інститут захисту інформації у хмарах яких досить розвинутий. Таким чином, воєнні обставини зумовили потребу у переосмисленні підходів до хмарних обчислень з акцентом на кіберстійкість та фізичну безпеку критичної інфраструктури. Цей досвід має бути корисним в подальшому розвитку стратегій як державних так і приватних щодо хмар не тільки в контексті фізичної та кібербезпеки, а й також організації, менеджменту й наявності плану дій стосовно даних на випадок кризових ситуацій. В ширшому контексті це, на мою думку, може зумовити не тільки в Україні, а й в світі, який базуватиметься на досвіді України, розвиток політики хмарного суверенітету, яка повинна ґрунтуватися на ризик-орієнтованому підході з орієнтуванням на випадок найменш сприятливого розвитку подій.

***

На основі даного розділу можна підвести такі підсумки:

1. На рівні ЄС відсутнє спеціальне регулювання, що стосується безпосередньо хмарних послуг, в тому числі щодо захисту персональних даних чи кібербезпеки при їх наданні. Тому правове регулювання в цій сфері відбувається в рамках загальних галузевих напрямків захисту персональних даних та кібербезпеки.

2. Центральним елементом регулювання захисту персональних даних у ЄС є Загальний регламент про захист даних (GDPR), який вважається одним з найсуворіших актів у цій сфері. Ключовою рисою GDPR є його екстериторіальність, через яку його положення поширюються на хмарних провайдерів по всьому світу, зокрема великих гравців як Amazon, Google та

Microsoft, якщо такі орієнтуються на ринок ЄС, змушуючи їх адаптувати свої глобальні стандарти діяльності відповідно до вимог цього регламенту

3. GDPR встановлює низку принципів захисту персональних даних, таких як законність, прозорість, точність, мінімізація даних тощо, які мають певні особливості застосування до хмарних послуг через їх технічну складність. Це змушує адаптувати хмарних провайдерів свої політики і підходи, як-от спрощувати свої публічні політики приватності під принцип прозорості.

4. В залежності від конкретних функцій і дій з даними, які виконуються, хмарні провайдери можуть виступати як контролери, процесори, спільні контролери чи субпроцесори персональних даних, що накладає на них різні вимоги та рівень відповідальності, що має уважно визначатися ними і їх клієнтами, якщо такі виступають контролерами. Загалом це демонструє регуляторну тенденцію на те, щоб зобов’язувати кожного, хто оброблює персональні дані і взаємодіє з хмарами, розуміти свою роль у такому ланцюжку передачі даних і вживати відповідних заходів, що сприяють дотриманню принципів GDPR.

5. GDPR встановлює суворі вимоги до передачі персональних даних до третіх країн через механізми адекватності, стандартні договірні умови та обов'язкові корпоративні правила. Ці правила загалом змушують як цілі юрисдикції, так і окремих суб’єктів хмарних послуг орієнтуватися на вимоги GDPR при співпраці з суб’єктами в ЄС, хоч фактично це може бути ускладнюватися практиками органів влади третіх країн.

6. Хмарні провайдери, як сильніші сторони у хмарних послугах і такі що мають набагато більше ресурсу, впроваджують практику "комплаєнс як послуга", тим самим перебираючи тягар своїх клієнтів-контролерів щодо низки організаційних обов’язків, які на них покладені GDPR. Розвиток цієї практики загалом позитивно сприймається органами ЄС, свідченням чого є затвердження EU’s Cloud Code of Conduct. Втім практика перебирання обов’язків контролерів хмарами як процесорами інколи є неприйнятною для деяких контролерів, які бажають більшого рівня контролю, як-от публічні органи влади.

7. Окремим питання окрім захисту персональних даних стоїть кібербезпека в контексті суспільно-важливих послуг. В цьому аспекті Директива ЄС 2022/2555 (NIS 2) відносить більшість хмарних провайдерів до категорії "основних суб'єктів" на рівні надавачів послуг енергетики чи охорони здоров’я, що свідчить при тенденцію визнання хмар, як зберігачів великої кількості даних в часи інформаційного суспільства, важливою інфраструктурою, що підлягає суворішому регулюванню кібербезпеки, включаючи заходи ex ante та ex post як-от політики інформаційної безпеки, обов'язкові оцінки ризиків, перевірки, аудити тощо.

8. Українське законодавство у сфері захисту персональних даних потребує вдосконалення, зокрема в частині ефективності застосування, контролю та санкцій, деяких нормативних визначень, що чіткіше регулює діяльність деяких учасників хмарних відносин тощо. В межах вирішення цієї проблеми очікується прийняття нових законів, які наблизять українські норми до стандартів GDPR.

9. Тенденцією української правової політики в контексті захисту даних у хмарних сервісах є розвиток публічного аспекту цього питання, зокрема на основі Закону України “Про хмарні послуги”, який встановлює строгі вимоги для хмарних договорів, коли вони стосуються публічного сектору та критичної інфраструктури. Воєнна агресія змусила Україну зосередитись на фізичній безпеці та кіберстійкості, що призвело до розвитку політик локалізації важливих даних та, за певних умов, до їх розміщення на хмарах за кордоном. Цей досвід може сприяти розвитку політики хмарної безпеки та “хмарного суверенітету”, базованої на ризик-орієнтованому підході.

РОЗДІЛ 3.
ЗАХИСТ ПРАВ СПОЖИВАЧІВ ТА ЦИФРОВОЇ КОНКУРЕНЦІЇ: ОСОБЛИВОСТІ І ТЕНДЕНЦІЇ ПРАВОВОГО РЕГУЛЮВАННЯ В КОНТЕКСТІ ХМАРНИХ ПОСЛУГ

3.1. Захист прав споживачів хмар як цифрових послуг: регуляторні тенденції

Аналогічно до персональних даних і безпеки даних у Європейському Союзі захист прав споживачів не регулюється окремо відносно хмарних послуг, а передбачає загальне галузеве законодавство особливості дії якого на хмарні послуги має вивчатися окремо.

Загалом характеризуючи тенденції регулювання захисту прав споживачів в контексті в хмарних послуг доцільно почати з ініціативи Європейської Комісії щодо перевірки відповідності права ЄС про захист прав споживачів на предмет цифрової справедливості. [50] В межах цієї ініціативи, Комісія оголосила про ініціативу перевірки того, чи потрібні додаткові дії для забезпечення однакового рівня справедливості онлайн і офлайн, фінальні результати якої очікуються в 2 кварталі 2024 року [51] Цю необхідність Комісія обґрунтовує зокрема посилаючись на дослідження, які вказують, що захист споживачів у цифровому світі має багато унікальних викликів, що потребує відповідних змін у регулюванні. [52] З одного боку, такі дослідження стосуються переважно більш активних дій, ніж звичайне надання хмарних послуг, як-от персоналізація в цифровому середовищі, яка впливає на їхній вибір та спотворює об’єктивне сприйняття ринку та світу загалом, аналіз поведінки в реальному часі для продажу продуктів, тощо. [53; с. 2-7] Водночас, варто зазначити, що навіть з таким пріоритетом, не варто виключати зміни щодо самих хмарних послуг, адже вже реалізовані зміни щодо цифрових послуг також дотично впливають на такі, а цифровий контент платформ типу SaaS може бути нерозривно поєднувати

хмарні та більш персоналізовані елементи (як-от електронний маркетинг та соціальні мережі).

Серед вже прийнятих актів ЄС, що регулюють захист прав споживачів у цифровій сфері, варто виділити директиву ЄС 2019/770 (відома як Директива «Про цифровий контент і цифрові послуги»). Хмарні послуги можна в основному за нею класифікувати як цифрові послуги, адже такі за визначенням «дозволяють споживачеві створювати, обробляти, зберігати або отримувати доступ до даних у цифровій формі», що і відповідає функціоналу хмари. [54; ст. 2(2)]

Стаття 3(1) цієї Директиви передбачає, що її дія розповсюджується не тільки при купівлі послуги, однак і при передачі персональних даних, окрім випадків коли така передача здійснюється виключно для цілей надання такої послуги. [54; ст. 3(1)] На мій погляд, ця умова є частиною вираженої тенденції, яка передбачає, що надання споживачем власних даних прирівнюється також до специфічної форми оплати, адже особливістю цифрового світу є усталена практика продажу даних покупців (в маркетологічних цілях тощо), що дозволяє отримувати дохід надавачу цифрових послуг.

Також, однією з проблем для споживача є питання відшкодування збитків у випадку порушення договору, зокрема якості та умов надання хмарних послуг, і Директива передає вирішення цього питання на розсуд держав-членів.[54; ст. 21] Однак, деякі дослідники критикують цей підхід, адже різні підходи до визначення шкоди і що можна нею вважати в різних країнах можуть ставити під загрозу ефективність стягнення такої. [55; с. 103-104] Я загалом, хочу погодитися з цією думкою і додати, що питання наскільки втрата даних (особливо, якщо дані не комерційні і їх вартість не можна визначити), відсутність доступу до них протягом періоду тощо можуть вважатися шкодою, є фактично що ключовими в контексті хмарних відносин і скоріш за все питання факту наявності шкоди за подібні порушення будуть ставати більш нагальними і можуть проявитися в подальшому розвитку правової політики ЄС.

На підкріплення до моєї думки, можна згадати й український підхід, закріплений в ст. 906(2) Цивільного Кодексу України, де вказано, що:

« Збитки, завдані невиконанням або неналежним виконанням договору про безоплатне надання послуг, підлягають відшкодуванню виконавцем у розмірі, що не перевищує двох неоподатковуваних мінімумів доходів громадян, якщо інший розмір відповідальності виконавця не встановлений договором.» [82; ст. 906(2)]

Це гарно ілюструє те, що в питанні відшкодування шкоди, передовий підхід про прирівнювання надання персональних даних до форми оплати може не застосовуватися, таким чином, обмежуючи можливості ефективного захисту, що надає Директива.

Ще однією особливістю Директиви «Про цифровий контент і цифрові послуги», яка є актуальною стосовно хмарних послуг, є те, що вона прописує не тільки суб'єктивні вимоги до цифрової послуги (як-от відповідність договору), а й об'єктивні, зокрема стаття 8(1)(b) встановлює, що послуга має

«мати таку кількість і володіти якостями та характеристиками продуктивності, у тому числі щодо функціональності, сумісності, доступності, безперервності та безпеки, які є звичайними для цифрового вмісту чи цифрових послуг того самого типу та яких споживач може розумно очікувати, враховуючи природу цифрового контенту або цифрової послуги…» [54; ст. 8(1)(b)]

Ця норма є істотною, якщо її оцінювати з призми того, що як було вказано в першому розділі, споживачі рідко читають умови самого договору про надання хмарних послуг (наприклад, terms of use) і не можуть самостійно вплинути на їх зміст, а лиш приєднуються до його умов. Цей принцип розумних очікувань є таким, що обмежує бізнес в тому як він може прописати умови договору тим, що загалом споживач може очікувати.

Все ж коли відношення і пріоритет об'єктивного чи суб'єктивного критерію за цією директивою є питанням спірним і не встановленим остаточно, то інша директива — 93/13/EEC відома як Unfair Terms Directive 1993 у статті 3(1) вказує, що

«Договірна умова, яка не була обговорена індивідуально, вважається несправедливою, якщо, всупереч вимозі добросовісності, вона спричиняє значний дисбаланс прав і обов'язків сторін, що випливають з договору, на шкоду споживачу.» [56; ст 3(1)]

Дослідники цього питання стверджують, що розвиток імплементації цієї норми великою мірою залежить від національних судових підходів і вказують, що загалом постачальник не може розроблювати договір виключно на власних бізнес-інтересах всупереч законним очікуванням споживача, якщо в споживача не було можливості вести перемовини щодо умов такого договору. [57; с. 790-791]

Аналізуючи ці норми, можна стверджувати, що вони загалом покликані забезпечити дотримання принципів добросовісності та розумних очікувань споживачів і відіграють ключову роль у встановленні більш справедливого балансу між правами та обов'язками сторін. Вони дозволяють оцінювати договірні умови не лише з формальної точки зору їх включення до тексту договору, а й з огляду на їхню відповідність об'єктивним стандартам справедливості та розумності. Такий підхід є доволі важливим у сфері цифрових послуг (в тому числі хмарних), де споживачі часто не повністю розуміють технічні деталі та наслідки певних договірних положень. Вимога, щоб послуги відповідали розумним очікуванням споживачів, встановлює своєрідний "захисний бар'єр" проти надто несприятливих і непрозорих умов. На мою думку, такі норми, які покликані забезпечити дотримання принципів справедливості та добросовісності, матимуть зростаюче значення у регулюванні відносин між великими постачальниками цифрових послуг і споживачами, адже це є необхідним кроком для подолання структурної нерівності в цій сфері та захисту прав і законних інтересів споживачів.

Закон України «Про цифровий контент та цифрові послуги» набув чинності 2 березня 2024 року і є прямим відповідником Директиви ЄС 2019/770. [98] Його норми будуть в першу чергу застосовуватися до хмарних послуг, оскільки як передбачено в статті 1(3) цього Закону дія положень Закону України "Про захист прав споживачів" поширюється на суб’єктів, визначених цим Законом тільки у частині відносин, не врегульованих цим Законом. [98; ст. 1(3)] В цьому контексті сам закон покриває ряд питань, які були вище визначені в як проблемні, як-от відповідність хмарних послуг як договору так і певним

об’єктивним критеріям, правові наслідки такої невідповідності тощо. [98; ст. 5, 6, 12] Це дає можливість стверджувати, що українське законодавство розвивається в бік кращого захисту споживачів, тим самим долаючи явну нерівність сторін у споживчому договорі хмарних послуг.

Іншою важливою особливістю тенденції регулювання захисту споживачів в умовах цифровізації відносин є збільшення актуальності додаткових способів захисту своїх прав. Загалом серед дослідників панує думка, що звернення до судової системи для захисту прав споживачів є обтяжливим та малопривабливим варіантом для більшості громадян. Судовий процес характеризується тривалістю, високою вартістю та потребує значних зусиль з боку позивача. Крім того, судовий процес потребує витрат часу та психологічних ресурсів, що часто не співмірні з ціною придбаного товару чи послуги, права щодо яких були порушені. Водночас, багато альтернативних методів є не настільки ефективними як хотілося б. Наприклад, Платформа ЄС для онлайн-врегулювання спорів (ODR) не гарантує успішного вирішення конфлікту, оскільки компанії не зобов'язані погоджуватися на процедуру альтернативного вирішення спору. У разі відмови постачальника від співпраці на платформі ODR, справа закривається через 30 днів без жодних подальших дій. Подібним чином, повноваження омбудсменів та споживчих організацій обмежені можливістю надавати рекомендації та консультації або ініціювати справи проти організацій безпосередньо, проте вони не мають важелів примусового виконання рішень на користь окремо взятих споживачів. [58; с. 242-247]

Вагомим кроком для вирішення цієї проблеми можна вважати Директиву 2019/2161, яка відома під назвою «The Omnibus Directive», яка вводить механізм індивідуальної компенсації у споживчі відносини. [59] Дослідники зазначають, що ця Директива, яка чітко вимагає від держав-членів забезпечити кожному споживачеві, який постраждав від недобросовісної комерційної практики, доступ до компенсації за завдану шкоду, зниження ціни та/або розірвання договору, є послідовним продовженням дії Директиви 2005/29/ЄС про недобросовісну комерційну практику, бо хоч остання створила дуже

прогресивну систему заборони недобросовісної комерційної практики у відносинах між бізнесом і споживачем, однак не забезпечила того, що якщо певна дія визнається недобросовісною практикою, то споживачі, що під неї потрапляли, мали б право на правовий захист від такої. [60; с. 75-76]

Іншим способом розвитку практики регулювання в бік покращення способів захисту своїх прав можна вважати прийняту в рамках ініціативи Європейської Комісії “New Deal for Consumers” Директиву 2020/1828 відому як Directive on Representative Actions. [61] Ця Директива спрямована на розвиток в процесуальному законодавстві держав-членів норм, які мають надати достатні можливості для представницьких позовних дій споживачів. Споживачі більше не повинні вступати в судовий процес самостійно, оскільки визначені кваліфіковані організації, такі як споживчі об'єднання чи державні органи, можуть ініціювати колективні позови від їхнього імені. Крім того, споживачі звільняються від відповідальності за судові витрати, за винятком надзвичайних обставин, що знімає додатковий тягар. Кваліфіковані організації наділені повноваженнями вимагати як заборонних заходів, так і компенсацій та інших форм відшкодування збитків на користь споживачів, яких вони представляють. [62] Отже, механізм колективних позовів за RAD значно посилює захист прав споживачів, надаючи їм доступ до ефективних засобів правового захисту через визначені організації без необхідності індивідуальної участі в судових процесах.

З іншого боку, деякі дослідники вважають, що з економічної точки зору колективні позови (груповий спосіб) є кращою альтернативою, ніж представницькі позови від імені споживачів кваліфікованими організаціями, як передбачено Директивою. При колективних позовах індивідуальні вимоги об'єднуються в одну справу, що забезпечує більш прямий зв'язок між позовом та збитками окремих споживачів. Це послаблює проблему принципал-агента, характерну для представницьких позовів споживчих організацій (яка може посилюватися через певну монопольність кваліфікованих організацій), які можуть не повністю відображати інтереси всіх постраждалих. [63]

Загалом, аналізовані директиви ЄС свідчать про чітку регуляторну тенденцію надання споживачам, як слабшій стороні у відносинах з хмарними провайдерами, більших можливостей для захисту своїх порушених прав. Виходячи з того, що звернення до судової системи часто є обтяжливим та недостатньо ефективним варіантом для пересічних споживачів, регулятори прагнуть запровадити додаткові механізми захисту, такі як право на компенсацію за недобросовісну практику бізнесу за фактом її встановлення або представницькі позови через спеціально уповноважені організації, що дозволяє відстоювати свої права більш оперативно та з меншими витратами ресурсів.

Однак паралельно з власне юридичними тенденціями щодо покращення можливості захисту прав споживачами, деякі дослідники виділяють в законодавстві і інструментарій захисту прав споживачів як “normative statement”. Він полягає в тому що великі компанії, зокрема хмарні як Amazon, намагаються дотримуватися законів різних країн, навіть якщо ці закони юридично їх не зобов'язують ефективно, оскільки це підвищує їхню репутацію та конкурентоспроможність. Ба більше, інколи такі хмарні провайдери добровільно надають споживачам у США права, гарантовані законодавством ЄС про захист прав споживачів, хоч безпосередньо в США вони не застосовні (з міркувань конкуренції, демонстрації «високих стандартів» чи уніфікації застосовних підходів), тим самим встановлюючи стандарти для своїх конкурентів, які теж змушені в США чи інших юрисдикціях встановлювати такий рівень захисту прав споживачів, який прямо законом там не вимагається.[58; с.238-242]

Таким чином, хоча нормативний вплив законів може зменшуватися через слабке правозастосування і в тому числі відсутність ефективного механізму відшкодування, репутаційні міркування спонукають великі компанії дотримуватися високих стандартів, визначених законами. Порівнюючи цю тенденцію із сферою захисту прав персональних даних, варто зазначити, що хоч GDPR передбачає куди ефективніший транскордонний механізм застосування свого стандарту (в межах правил передачі даних до третіх країн), який відсутній в праві захисту прав споживачів, втім і в контексті останнього доцільно

стверджувати, що норми і тенденції, що запроваджуються в ЄС мають великий вплив на відповідні практики у всьому світі.

Іншою проблемою, яка постає, є захист питання спадкування даних та/або облікового запису в хмарі. Це право, з одного боку, не є частиною сфери прав споживачів, а скоріш є окремою сферою цивілістики, однак в контексті хмарних послуг, на відміну від класичного спадкування, основне питання, як було оглянуто в першому розділі, постає в тому, чи надасть хмарний провайдер доступ до даних спадкоємцям. Це залежить, як відомо, зокрема від умов договору між провайдером та клієнтом, але оскільки споживач майже завжди ніяк не впливає на умови договору, то постає питання того, чи не є така умова несправедливою стосовно такого споживчого договору, що загалом варто розглядати з призми права захисту прав споживачів.

Загалом, як було зазначено в першому розділі, питання спадкування даних у хмарі (особливо, якщо така робиться без заповіту чи іншої волі спадкодавця) передбачає дуже специфічний конфлікт інтересів між спадкоємцями, спадкодавцем та хмарним провайдером, балансування якого потребує нормативного вирішення для правильного збалансування таких інтересів.

Дослідники зазначають, що питання спадкування хмарних облікових записів та/або даних є питанням дискусійним. Одним із аргументів є те, що такі можуть містити конфіденційну та особисту інформацію, розголошення якої може порушити право на приватність як самого користувача, так і третіх осіб, з якими він взаємодіяв. [64; с. 237-240] Інші дослідники вказують, що попри те, що європейська система побудована на принципі універсального спадкоємництва, що означає, що нематеріальні активи мають спадкуватися орієнтовно на рівні з матеріальними, однак в контексті облікових записів це має певні обмеження. Це пов’язано з тим, що облікові записи мають і особистий фактор (особливо в контексті соціальних мереж), повне успадкування такого активу з правом публікувати від імені померлого видається етично сумнівним. [65; с. 16-18]

Знаковою справою в цьому контексті є справа відома за назвою LG Berlin Facebook case *(Landgericht Berlin, Urteil vom 17.12.2015, Az. 20 O 172/15*.). У цій справі після самогубства 15-річної дівчини її батьки намагалися отримати доступ до її облікового запису в Facebook, щоб з'ясувати деталі трагедії. Однак, Facebook відмовив у доступі, посилаючись на політику конфіденційності та наданню обліковому запису меморіального статусу. Німецький суд постановив, що згідно з принципом універсального правонаступництва, обліковий запис є частиною спадщини і має успадковуватись спадкоємцями, незважаючи на положення користувацької угоди Facebook про неможливість передачі облікового запису. [65; с. 19-21] [66]

Суд визнав недійсними положення договору між Facebook та користувачем, які унеможливлювали передачу облікового запису у спадщину. Зокрема, умова договору про надання послуг, яка перетворювала сторінку на меморіальний статус після смерті користувача, позбавляючи спадкоємців доступу до даних, була визнана такою, що необґрунтовано обмежує права іншої сторони договору. [65; с. 20]

Деякі доктриналісти вважають, що є доцільним надавати перевагу інтересам спадкоємців щодо доступу до цифрових активів померлої особи над обмеженнями, встановленими умовами користування (terms of use) хмарних провайдерів. Це міркування ґрунтується на кількох ключових аргументах. По-перше, відсутність вираженого розпорядження спадкодавця може свідчити як про бажання зберегти приватність, так і про відсутність чіткої позиції з цього питання. По-друге, забезпечення спадкоємцям права доступу до цифрових активів може сприяти збереженню матеріалів, які в іншому випадку могли б бути втрачені, а також активів, що становлять суспільний або культурний інтерес. Нарешті, такий підхід буде співмірним з правом власності на фізичні активи, стверджуючи, що спадкоємці мають отримувати доступ до цифрових активів у разі відсутності заповіту. [67; с. 205-206]

Хоч в межах країн ЄС можна стверджувати про певне превалювання підходу недискримінації джерела спадкування (який в контексті хмарних

сервісів означає, що характер відносин і умови договору між хмарним провайдером і клієнтом, не можуть змінювати порядок спадкових відносин, адже неправомірно порушують законні спадкові права осіб), однак такий тільки закріплюється в законодавстві окремих країн щодо цифрових послуг. Тому серед дослідників існує позиція, наразі доречним проаналізувати таку практику з метою розробки єдиного підходу на рівні ЄС, інакше існує небезпека поглиблення розбіжностей між національними правовими системами держав-членів ЄС у цій галузі, що значно ускладнить неминучий процес гармонізації правового регулювання в майбутньому. [65; с. 38]

Отже, можна підсумувати, що, як я зазначав, питання спадкування, яке традиційно не має відношення до захисту прав споживачів, в контексті хмарних послуг постало з таким досить тісним зв'язком в контексті несправедливих умов споживчого договору: фактично наявні умови надання хмарних послуг нерідко передбачають визначення долі облікового запису та даних особи після її смерті, що можна розцінювати як надмірне обтяження спадкових прав, які мають визначатися волею особи та законодавством та не можуть дискримінуватися на підставі положень, встановлених постачальниками хмарних послуг в умовах користування. Тому, я вважаю, що враховуючи все більше значення у світі цифрових даних, ця невизначеність має бути врегульована спеціальним законодавством, скоріш за все, віддаючи належне принципу субсидіарності, навіть на рівні ЄС, інакше передача даних залежатиме від політики хмарних компаній, а не від принципів спадкового права, що є неприпустимим. Водночас, я не можу повністю погодитися з думкою, що спадкоємці завжди повинні мати доступ до даних спадкодавця (як-от до матеріального його майна), адже це не завжди відповідало б його бажанню, а скоріш вважаю, що правова політика має більш комплексно підходити до цього питання і будуватися зокрема на тому, щоб розробляти інструментарій спонукання і спрощення надання власної позиції щодо цього питання спадкоємцем за життя. В будь-якому випадку, можна вважати, що порядок спадкової передачі облікових записів і інформації, є

питанням, яке все актуальніше ставатиме перед правовим регулюванням в контексті хмарних послуг.

3.2. Правове регулювання цифрової конкуренції: аспект хмарних послуг

Наступним питанням в контексті хмарних послуг, регулювання якого наразі активно встановлюється і досліджується, є цифрова конкуренція. Хоч, як відомо, в ЄС є окремий інститут антиконкурентних норм (як-от похідних від ст. 102 ДФЄС), однак він не є об’єктом огляду в межах цієї роботи, адже загалом традиційні інструменти антимонопольного регулювання не є пріоритетними у застосуванні на цифрових ринках, надаючи більш активну роль наразі спеціальним новоприйнятим актам, які регулюють питання конкуренції цифрових надавачів послуг, орієнтуючись на властиву їм специфіку. [68] Відтак, надалі я розгляну такі оглянувши такі акти як Digital Services Act (DSA), Digital Markets Act (DMA) та Data Act. Водночас, коли останні два є широковизнані, як ті що включають антиконкурентну сферу, то DSA такої майже немає, однак підпадає під загальну тенденцію регулювання великих надавачів цифрових послуг в ЄС, тож також вартий розгляду для кращого розуміння контексту.

Закон про цифрові послуги (DSA) (Regulation (EU) 2022/2065) є актом, що надає новий комплекс єдиних норм на рівні ЄС, спрямованих на регламентацію діяльності платформ онлайн-посередників, що забезпечують споживачам доступ до товарів, послуг та контенту, норми якого остаточно почали застосовуватися з 17 лютого 2024 року. [69] [70] Ключовим нововведенням є певні обов’язки, що накладаються на такі платформи посередники. Прикметно, що хмарні провайдери, якщо вони не виконують інші функції, мають куди менше обов’язків ніж більшість інших онлайн-платформ (як-от соціальні платформи і пошукові системи), адже відносяться за розподілом до статусу надавачів послуг хостингу. [71] Відтак, за хмарними провайдерами закріплюються певні обов'язки, такі як: призначення єдиних контактів для взаємодії з органами влади та одержувачами

послуг, забезпечення прозорості положень щодо процедур модерації контенту на платформі (заборони публікації незаконного або неприйнятного згідно з правилами сервісу контенту, можливих заходів реагування), щорічна публікація звітів про прозорість здійснених заходів модерації контенту, обов'язок повідомляти про підозри у вчиненні злочинів, що становлять загрозу життю чи безпеці осіб, запровадження процедур повідомлення та реагування на нелегальний контент, що зберігається на сервісі, тощо. [72] Таким чином, даним актом створюються механізми підзвітності та прозорості функціонування хмарних платформ.

Однак, в контексті хмарних сервісів, як пишуть фахівці, застосування DSA може викликати певні складнощі, як-от у випадках використання хмарних сервісів SaaS, коли зазвичай клієнт має прямий контроль над власним контентом. Зокрема, якщо хмарний провайдер виявляє незаконний або шкідливий контент на веб-сайті клієнта, який розміщений у хмарному середовищі, то провайдер може заблокувати доступ лише до всього сервера загалом, але не має можливості отримати доступ та видалити окремі частини неналежного контенту, тобто виконати свій обов’язок до DSA. [73]

З такою думкою можна погодитися, однак як було описано в першому розділі, клієнт має дуже великий рівень контролю, якщо послуги надаються за схемою IaaS, що обтяжує хмарні платформи у виконанні модераційних обов’язків за DSA. Тому можна зробити висновок, що DSA, надаючи найбільше положень щодо регулювання платформ типу SaaS, які окрім хмарної виконують функції соціальних мереж, пошукових систем тощо, хоч і юридично покриває, однак, на мій погляд, все ж залишає поза фокусом менш подібні до вказаного типу хмарні сервіси.

Попри те, що DSA дає загальні інструменти над контролем і підзвітністю щодо домінуючих хмарних провайдерів, все ж інструменти безпосередньо на захист цифрової конкуренції надаються іншими двома ключовими актами — Digital Markets Act (DMA) та Data Act.

Digital Markets Act (DMA, Regulation (EU) 2022/1925) встановлює гармонізовану регуляторну основу для ключових цифрових платформних сервісів, з метою підвищення їх конкурентності та справедливості для кінцевих та бізнес-користувачів. [74; с. 41]

DMA доповнює законодавство ЄС у сфері конкуренції, оскільки останнє виявилося недостатнім для вирішення проблем у цифрових ринках через обмежену сферу застосування ст. 102 ДФЄС, необхідність ретроспективного аналізу та складність case-by-case підходу. Загалом, Регулювання DMA фокусується на ключових платформних сервісах (CPS), де значні масштабні ефекти, мережеві ефекти та перевага в даних можуть негативно впливати на справедливість та конкурентність на всьому ринку. DMA визначає "гейткіперів" (gatekeepers) – компанії, що надають CPS у щонайменше трьох державах-членах ЄС та відповідають кількісним і якісним критеріям суттєвого впливу на внутрішній ринок та сталого ринкового домінування. На "гейткіперів" накладається 21 пряма заборона певних практик, спрямована на системне підвищення конкурентності та справедливості, без необхідності доведення їх негативного впливу в кожному конкретному випадку. [74; с. 41-43] Ці заборони передбачені в статтях 5 та 6 DMA, та загалом включають дії, які передбачають зловживання своїми фінансовими, ринковим та технічними можливостями для практик, які обмежують конкуренцію, як-от вимога дозволяти та технічно забезпечувати встановлення та ефективне використання сторонніх програмних додатків або магазинів додатків на операційній системі гейткіпера або вимога дозволяти та технічно забезпечувати легке видалення будь-яких програмних додатків на операційній системі гейткіпера, за винятком тих, що є суттєвими для її функціонування. [75; ст. 5, 6] На мою думку, такі обмеження потенційно антиконкурентних дій ex-ante (замість класичної оцінки впливу на ринок на кожен окремий випадок ex-post) для певної групи суб’єктів є унікальним способом врегулювання щодо цифрових послуг, що є відповіддю регуляторів на нові виклики для конкуренції у такому середовищі.

Якщо характеризувати особливості впливу DMA на саме хмарні послуги, то варто зазначати, що такі за визначенням також визнаються CPS і відповідно можуть бути визнані гейткіперами. [75; ст. 2(2)(i)] Однак дослідники зазначають про певні перешкоди в ефективній застосовності всіх вимог щодо гейткіперів до провайдерів хмарних послуг. По-перше, концепція визначення провайдера хмарних послуг як гейткіпера є проблематичною, оскільки хмарні послуги є однобічними, а не двосторонніми платформами, що ускладнює застосування поняття "важливого шлюзу" (important gateway) до них, а це важливо, адже це одна з умов набуття статусу гейткіпера відповідно до статті 3(1)(b) DMA. Крім того, відсутність мережевих ефектів для хмарних послуг також ставить під сумнів їх визначення як важливого шлюзу. [74; с. 43-47] По-друге, навіть саме визначення бізнес-користувачів і кінцевих користувачів (а саме між ними виступає CPS важливим шлюзом) хмарних послуг також є проблематичним, оскільки, як розглядалося в першому розділі, такі бізнес-користувачі, як правило є іншими хмарними провайдерами, що формують ланцюжок між «найвищим» в ланцюжку хмарним провайдером і користувачем, коли в DMA гейткіперу передбачається функція скоріш посередника між користувачем та бізнес-користувачем, а не вищою ланкою вертикального ланцюжка. По-третє, навіть якщо провайдер хмарних послуг буде визначений як гейткіпер, застосовність до нього зобов'язань за статтями 5 та 6 DMA викликає невизначеності, оскільки ці вимоги можуть мати інший сенс для хмарних послуг порівняно з двосторонніми платформами. [74; с. 43-47] Як бачимо на практиці, Європейська Комісія серед списку гейткіперів визначила виключно двосторонні CPS і жодної безпосередньо хмарної послуги. [76]

Отже, можна зробити висновок, що хоч DMA є передовим актом захисту цифрової конкуренції, який суттєво змінює класичні антконкурентні догми, втім сама його основа поки що надто нечітко сформована для безпосередньо хмарних послуг. На мою думку, у разі вдалого застосування норм DMA до нішових двосторонніх платформ, які є все ж центральним об’єктом регулювання цього

акту, можна очікувати і подальше більш чітке розширення дії подібних інструментів щодо безпосередньо хмарних послуг.

Іншим актом сфери цифрової конкуренції, який впливає на хмарні послуги є Data Act (Regulation (EU) 2023/2854), норми якого почнуть застосовуватися з вересня 2025 року та який має за центральну мету сприяння конкурентоспроможному ринку даних. [78] Розглядаючи цей елемент як частину сучасної антиконкурентної політики, варто зауважити, що вільний рух даних розглядається як фундамент становлення єдиного цифрового простору ЄС, де дані, як життєво важливий ресурс для економічного зростання, конкурентоспроможності та інноваційного розвитку, можуть бути повноцінно залучені й використані, а безперешкодний обіг даних постав новим викликом європейської політики, спрямованої на сприяння розвитку інноваційних продуктів і послуг, тісно пов'язаних із вподобаннями споживачів. [74; с. 24]

Першим заходом в контексті конкурентності даних є шостий розділ акту, який встановлює мінімальні вимоги до хмарних контрактів щодо сприяння швидкому та безперешкодному переходу клієнтів між провайдерами послуг обробки даних без втрати даних чи функціональності. Крім того, з часом Акт повністю забороняє плату за перехід, включаючи плату за вивід даних.[77]

Інший захід встановлений восьмим розділом, що передбачає розвиток глобальної інтерперабельності даних, зокрема зобов’язання здійснювати доступний опис та гармонізацію стандартів і відкритих специфікацій взаємодії хмарними провайдерами, що є ключовим для полегшення переходу клієнтів між ними. Європейська Комісія оцінюватиме перешкоди для взаємодії та визначатиме пріоритети стандартизації, на основі чого за потреби розроблятимуться спільні технічні специфікації за участі зацікавлених сторін. [77]

Зрештою, у четвертому розділі Data Act передбачає заходи для захисту всіх європейських підприємств, особливо малих і середніх, від несправедливих договірних умов у відносинах між хмарним провайдером і таким підприємством. Зокрема, Акт встановлює перелік умов, які презюмуються як несправедливі,

якщо вони нав'язуються однією стороною в односторонньому порядку. Такі несправедливі умови можуть бути виключені або обмежені, що спрямовано на виправлення нерівності у відносинах між постачальниками (наприклад, великими хмарними провайдерами) та їхніми клієнтами. [77]

На мій погляд, такі заходи, які впроваджує Data Act, є дієвим способом захисту конкуренції на ринку даних, що передбачає, в контексті хмарних послуг, легку зміну провайдерів, можливість легко поєднувати послуги кілька хмарних провайдерів і бути менш залежним від кожного з них. Важливим аспектом є застосування такого інституту як несправедливі умови договору у відносинах, де відсутні споживачі як такі, що розширює певний захист також і на малі та середні підприємства, які часто теж потерпають від майже одностороннього домінування сторони хмарного провайдера у договірних відносинах, про яке зазначалося в першому розділі.

***

На основі даного розділу можна підвести такі підсумки:

1. У ЄС захист прав споживачів та цифрова конкуренція щодо хмарних послуг не регулюються окремо, а передбачають загальне галузеве законодавство, особливості дії якого на хмарні послуги має предметом окремого вивчення. Також в правовій політиці ЄС можна виділити ключову тенденцію здійснювати аналіз специфічних загроз щодо прав споживачів, що виникають саме в цифровому середовищі, та регуляторно реагувати на ці виклики.

2. Директива ЄС 2019/770 («Про цифровий контент і цифрові послуги») класифікує хмарні послуги як цифрові послуги та передбачає, що надання споживачем власних даних (окрім цілей безпосереднього виконання договору) прирівнюється до оплати, що є базовою причиною, чому стандарти захисту прав споживачів застосовуються практично до всіх хмарних сервісів. Однак, не вирішеним є питання відшкодування збитків у випадку порушення договору про надання хмарних послуг, що залишає його на розсуд держав-членів, коли

розвиток захисту прав споживачів потребує формування універсальних підходів до врегулювання цього питання і відповідної подальшої гармонізації.

3. Директива ЄС 2019/770 встановлює об'єктивні вимоги до цифрових послуг, зокрема принцип розумних очікувань споживачів, який обмежує бізнес у формулюванні умов договору. Директива 93/13/ЕЕС передбачає, що договірна умова, яка не була обговорена індивідуально та спричиняє значний дисбаланс прав і обов'язків сторін на шкоду споживачу, вважається несправедливою. Це загалом свідчить про тенденцію відмовлятися від розгляду договору про надання хмарних послуг, як такого, що є вираження волі двох осіб (адже де-факто таким він не є в більшості випадках) і розглядати його скоріш з позицій об’єктивної відповідності.

4. Також наявна тенденція до розширення способів захисту прав споживачів хмарних послуг, адже виключно судові та класичні позасудові способи мають ряд недоліків і не є завжди ефективними для споживача. Зокрема, директива 2019/2161 та Директива 2020/1828 спрямовані на розвиток додаткових способів захисту прав споживачів, таких як право на компенсацію за недобросовісну практику бізнесу та представницькі позови через спеціально уповноважені організації.

5. Українське законодавство також адаптується до європейських підходів та тенденцій, спрямованих на кращий захист прав споживачів хмарних послуг, про що зокрема свідчить прийняття Закону України "Про цифровий контент та цифрові послуги".

6. Великі хмарні компанії, як Amazon, намагаються дотримуватися законів про захист прав споживачів різних країн, навіть якщо ці закони юридично мають складнощі в застосуванні, роблячи це з репутаційних міркувань та для підвищення конкурентоспроможності. Також, норми і тенденції, що запроваджуються в ЄС, мають великий вплив на відповідні практики у всьому світі, адже часто вважаються кращими практиками, які великі компанії повсюдно переймають для цілей репутації, конкуренції чи уніфікації.

7. Питання спадкування облікових записів та даних у хмарі є дискусійним і потребує нормативного врегулювання для збалансування інтересів спадкоємців, спадкодавця та хмарного провайдера. Загалом, існує тенденція в думці доктриналістів і практиках окремих країн, що умови договорів з хмарними провайдерами не можуть дискримінувати спадкові права осіб, що згодом може постати актуальним питанням на рівні регулювання ЄС.

8. У контексті хмарних послуг традиційні інструменти антимонопольного регулювання не є пріоритетними, надаючи більш активну роль спеціальним новоприйнятим актам, які спеціалізуються на цифровій конкуренції, таким як Digital Markets Act (DMA) та Data Act.

9. Digital Markets Act (DMA) встановлює гармонізовану регуляторну основу для ключових цифрових платформних сервісів, однак його застосування до безпосередньо хмарних послуг є проблематичним через їх специфіку, відмінну від двосторонніх платформ. Також проблематичним застосування до хмар є застосування Digital Services Act (DSA), який теж фокусується більше на двосторонніх платформах (як-от соціальні мережі). Це загалом підводить до висновку що сучасні правотворчі і правозастосовні тенденції, хоч і розглядають хмарні сервіси в контексті цифрової конкуренції, але такі затьмарюються більш ризиковими в цьому питанні цифровими послугами, які наразі мають набагато більш активну увагу з боку регуляторних органів.

10. Data Act, який має почати застосовуватися у 2025 році, спрямований на сприяння утворенню конкурентоспроможному ринку даних шляхом встановлення вимог до хмарних контрактів, розвитку інтероперабельності даних та захисту малих і середніх підприємств від несправедливих договірних умов у відносинах з хмарними провайдерами. Це розкриває тенденцію розвитку ще одного цифрового антиконкурентного напряму — ринку неперсональних даних.

ВИСНОВКИ

В межах даної роботи можна здійснити наступні висновки:

1. Хмарні послуги широко увійшли в повсякденне життя сучасного суспільства включаючи як функціонування організацій різного масштабу, так і повсякденне життя людей. В розрізі зростання значення інформації у світі часто сталість і надійність роботи хмарних сервісів має все більш критичне значення. Однак ринок хмарних послуг характеризується домінуванням кількох великих провайдерів, що призводить до явної нерівності договірних відносин з більшістю клієнтів. Така ситуація зумовлює необхідність ефективного правового регулювання цієї сфери, яке б могло забезпечувати прозорість і запобігати можливим зловживанням з боку хмарних провайдерів як домінуючої сторони у таких відносинах.

Для розробки таких регуляторних заходів важливим є детальне вивчення особливостей хмарних послуг та всієї складності відносин, що виникають у цій сфері. Зокрема, хмарні послуги за своєю правовою природою характеризуються постійним і безперешкодним доступом користувачів до обчислювальних ресурсів провайдерів задля зберігання власних даних, іншими ознаками, що вирізняють їх від інших цифрових послуг, різними моделями розподілу контролю (IaaS, PaaS, SaaS) та можливістю формування складних ланцюжків надання послуг. Ці характеристики породжують низку актуальних проблем, серед яких — розподіл відповідальності, забезпечення прав користувачів, врегулювання питань успадкування даних, фрагментації даних, прозорості договірних умов тощо. Вирішення таких питань вимагає збалансованого правового підходу, спрямованого на захист прав споживачів, персональних даних, конкуренції та безпеки даних, який не може бути досягнутий виключно умовами договору, а вимагає цілої низки заходів правової політики, формування якої задає сучасні тенденції правового регулювання хмарних послуг.

2. Регулювання захисту персональних даних при наданні хмарних послуг у ЄС значною мірою ґрунтується на Загальному регламенті про захист даних

(GDPR) як основному нормативно-правовому акті у цій сфері. Втім, застосування GDPR до складних хмарних систем залишає певні виклики, зокрема щодо реалізації окремих принципів обробки персональних даних та визначення ролей суб'єктів (контролерів, спільних контролерів, процесорів, субпроцесорів) у таких відносинах. Вирішення цих питань вимагає як від хмарних провайдерів розробки відповідних політик, стратегій і оцінки у кожному конкретному випадку, так і від регуляторів подальшого розвитку та адаптації законодавства під специфіку хмарних послуг.

Водночас, спостерігається тенденція, коли організаційно та фінансово сильні хмарні провайдери проактивно перебирають на себе функцію забезпечення комплаєнсу за GDPR ("комплаєнс як послуга"), що в цілому позитивно сприймається регуляторами, про що свідчить прийняття ними актів, як-от EU's Cloud Code of Conduct. Більше того, екстериторіальна дія GDPR поширює його вимоги на суб'єктів за межами ЄС, що змушує хмарних провайдерів у всьому світі адаптувати свої політики захисту персональних даних відповідно до стандартів цього регламенту.

У сфері кібербезпеки хмарні послуги також набувають важливого значення, що підтверджується віднесенням більшості хмарних провайдерів до категорії "основних суб'єктів" згідно Директиви ЄС 2022/2555 (NIS 2). Це свідчить про тенденцію визнання хмар як важливої інфраструктури, що зумовлює необхідність суворішого регулювання в цій сфері, включаючи вимоги до політик інформаційної безпеки, оцінки ризиків, перевірок, аудитів тощо.

3. Сфера захисту прав споживачів та захисту конкуренції наразі в багатьох аспектах активно переосмислюються, що зокрема пов’язано з цифровізацією економіки. Стосовно хмарних послуг тенденція проявляється у кількох аспектах, як-от розширення поняття оплати в цілях захисту прав споживачів відповідно до реалій цифрової економіки, де оплатою можна вважати і передачу персональних даних в обмін на хмарну послугу, розширення способів захисту прав споживачів хмарних послуг, як-от що передбачені Директивою 2019/2161 та Директивою 2020/1828 право на компенсацію за недобросовісну торгову практику та

представницькі позови через уповноважені організації, встановлення і розвиток практики об'єктивних вимог до цифрових послуг, що зменшує можливості хмарних провайдерів зловживати типовими умовами договорів. Також є низка назрілих, хоч ще не вирішених питання, як-от формування політики ЄС щодо умов контрактів, які безпідставно беруть на себе повноваження розпоряджатися спадковими правами користувачів щодо контенту, який знаходиться на хмарі.

Водночас, норми й тенденції, запроваджувані в ЄС, отримують глобальний вплив на всі світові юрисдикції, оскільки часто вважаються кращими практиками, яких великі хмарні компанії впроваджують задля репутації, конкуренції чи уніфікації.

У контексті хмарних послуг традиційні інструменти антимонопольного регулювання поступаються місцем спеціальним актам, таким як Digital Markets Act (DMA) та Data Act, які спрямовані на регулювання цифрової конкуренції, зокрема нормативного попередження антикокурентних дій (DMA) або формування нового виміру антиконкурентного напряму — ринку неперсональних даних (Data Act). З іншого боку, варто зазначити, що сучасні правотворчі й правозастосовні тенденції приділяють більшу увагу двостороннім цифровим платформам (як-от соціальні мережі), тоді як хмарні послуги залишаються поза авангардом правової політики, хоча й включені до сфери регулювання зазначених актів, а також інших актів, які збільшують цифрову прозорість (як-от Digital Services Act), що робить практику їх застосування до хмарних послуг очікуваною в перспективі (та після того, як деякі акти врахують особливості хмарних послуг серед інших цифрових послуг, як-от відсутність посередницької ролі).

4. Тривалий час відсутність спеціального регулювання в Україні спричинило дискусії щодо приватно-правової природи договорів хмарних послуг, однак дійшовши до загалом прийнятого висновку, що хмарний договір є договором про надання послуг, наразі основна увага скоріш зміщується до питання не того, що таке хмарні послуги, а того, які ризики вони несуть і як їх

ефективно врегулювати, тому саме ці питання становитимуть основу тенденцій розвитку правового регулювання хмарних послуг в Україні.

Сучасна українська правова політика характеризується розвитком публічно-правового регулювання хмарних послуг, зокрема у зв’язку з прийняттям закону «Про хмарні послуги», який дає низку вимог у хмарних відносинах B2G. Ще більше тенденцію до формування державної політики у сфері хмарних послуг зумовила російська агресія, яка поставила актуальними питання безпеки критичних державних інформаційних систем і національної стратегій у цій сфері. Другою тенденцією регулювання хмарних послуг в Україні є рух галузевого законодавства до вимог ЄС. Зокрема, законодавство про захист персональних даних, яке для ефективної дії потребує вдосконалення, перспективно буде замінене новими законами, які наблизять українські норми до стандартів GDPR. Це застосовно і до захисту прав споживачів хмарних послуг: як-от набрання чинності закону "Про цифровий контент та послуги" також адаптує споживче законодавство до норм законодавства ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cloud Computing Statistics (How Many Companies Use Cloud Computing?). *Colorlib*. URL: https://colorlib.com/wp/cloud-computing-statistics/ (дата звернення: 05.03.2024).

2. Duarte F. Percent of Corporate Data Stored in the Cloud (2024). *Exploding Topics*. URL: https://explodingtopics.com/blog/corporate-cloud-data (дата звернення: 05.03.2024).

3. Cloud Storage Statistics You Need To Know. *Connectbit*. URL: https://connectbit.com/cloud-storage-statistics/ (дата звернення: 05.03.2024).

4. Cloud computing - statistics on the use by enterprises - Statistics Explained. *European Commission*. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises (дата звернення: 07.03.2024).

5. Hava T. 2024 Cloud Market Share Analysis: Decoding Industry Leaders and Trends. *Azure, GCP, Kubernetes and AWS Diagrams Automated | Hava*. URL: https://www.hava.io/blog/2024-cloud-market-share-analysis-decoding-industry-leaders-and-trends (дата звернення: 07.03.2024).

6. Cloud Computing in 2024 & Top 10 Cloud Service Providers. *Tridens*. URL: https://tridenstechnology.com/cloud-service-providers/ (дата звернення: 07.03.2024).

7. 800-145. The NIST Definition of Cloud Computing. Effective from 2012-04-27. Official edition. 7 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (дата звернення: 07.03.2024).

8. Westbrook N. European Data Protection Law and Practice / ed. by E. Ustaran. International Association of Privacy Professionals (IAPP), 2019.

9. IaaS vs. PaaS vs. SaaS - Differences, Examples and Diagram | LeanIX. LeanIX | Enterprise Architecture Transformation. URL:

https://www.leanix.net/en/wiki/apm/iaas-vs-paas-vs-saas (дата звернення: 25.03.2024).

10. Views From The Cloud: A History of Spotify's Journey to the Cloud, Part 1 - Spotify Engineering. Spotify Engineering. URL: https://engineering.atspotify.com/2019/12/views-from-the-cloud-a-history-of-spotifys-journey-to-the-cloud-part-1-2/ (дата звернення: 25.02.2023).

11. Kemp R. Cloud services: due diligence issues | Practical Law. *Practical Law*. URL: https://uk.practicallaw.thomsonreuters.com/9-573-0466?transitionType=Default&contextData=(sc.Default)&firstPage=true (дата звернення: 25.02.2023).

12. Michels, Johan David and Millard, Christopher and Turton, Felicity, Contracts for Clouds, Revisited: An Analysis of the Standard Contracts for 40 Cloud Computing Services (June 11, 2020). Queen Mary School of Law Legal Studies Research Paper No. 334/2020. URL: https://ssrn.com/abstract=3624712 (дата звернення: 25.02.2023).

13. Beyond the Clouds, Part 1: What Cloud Contracts Say About Who Owns and Can Access Your Content. *Search eLibrary : SSRN*. Queen Mary School of Law Legal Studies Research Paper No. 315/2019. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386609 (дата звернення: 26.03.2024).

14. Hon, W. Kuan and Millard, Christopher and Singh, Jatinder, Cloud Computing Demystified (Part 1): Technical and Commercial Fundamentals (February 2022). URL: https://ssrn.com/abstract=4030064

15. Benoliel, Uri and Becher, Shmuel I., The Duty to Read the Unreadable (January 11, 2019). 60 Boston College Law Review 2255 (2019), URL: https://ssrn.com/abstract=3313837

16. Sandle T. Report finds only 1 percent reads 'Terms & Conditions' (January 20, 2020). Digital Journal. URL: https://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127 (дата звернення: 26.03.2024).

17. Bickerstaff R. Cloud services: overview | Practical Law. *Practical Law*. URL: https://uk.practicallaw.thomsonreuters.com/4-566-3285?transitionType=Default&contextData=(sc.Default) (дата звернення: 27.03.2024).

18. What is GDPR, the EU's new Data protection law?. GDPR.eu. URL: https://gdpr.eu/what-is-gdpr/ (дата звернення: 27.03.2024)

19. Does the GDPR apply to companies outside of the EU?. GDPR.eu. URL: https://gdpr.eu/companies-outside-of-europe/ (дата звернення: 27.03.2024)

20. Determann L. Determann's Field Guide to Data Privacy Law. 5th ed. Edward Elgar Publishing Limited, 2022

21. Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR). General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/art-5-gdpr/ (дата звернення: 28.03.2024).

22. Art. 4 GDPR – Definitions - General Data Protection Regulation (GDPR). General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/art-4-gdpr/ (дата звернення: 28.03.2024).

23. Justice and Consumers Article 29 - guidelines on transparency under regulation 2016/679 (wp260rev.01). European Commission. URL: https://ec.europa.eu/newsroom/article29/items/622227 (дата звернення: 28.03.2024).

24. Kamarinou, Dimitra and Millard, Christopher and Turton, Felicity, Protection of Personal Data in Clouds and Rights of Individuals (May 2021). Chapter 8, 'Protection of Personal Data in Clouds and Rights of Individuals', in C. Millard (ed.) Cloud Computing Law, (2nd edn, OUP 2021, URL: https://ssrn.com/abstract=4255833

25. Google Cloud Platform Subprocessors. Google Cloud. URL: https://cloud.google.com/terms/subprocessors (дата звернення: 28.03.2024).

26. Guidance on the use of cloud computing. UK Information Commissioner's Office. 20121002 Version: 1.1. October 2012 URL: https://ico.org.uk/media/about-the-ico/documents/1042330/cloud-computing-guidance-for-organisations.pdf

27. Загальний регламент про захист даних (GDPR) - GDPR-Text.com. GDPR-Text.com - GDPR Text, Translation and Commentary. URL: https://gdpr-text.com/uk/ (дата звернення: 30.03.2024).

28. Art. 20 GDPR – Right to data portability - General Data Protection Regulation (GDPR). General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/art-20-gdpr/ (дата звернення: 29.03.2024).

29. Data mobility and the future of hypercloud. Gartner Peer Insights. URL: https://www.netapp.com/media/72898-Netapp_2022-06-13_Data_Mobility_and_the_Future_of_Hypercloud_v4-92.pdf. (дата звернення: 29.03.2024).

30. EDPB provides guidance on the concepts of controller and processor in the GDPR (Part I). *Tech Law Blog*. URL: https://www.techlaw.ie/2021/08/articles/data-protection/edpb-provides-guidance-on-the-concepts-of-controller-and-processor-in-the-gdpr-part-i/ (дата звернення: 29.03.2024).

31. Kamarinou, Dimitra and Millard, Christopher and Turton, Felicity, Responsibilities of Controllers and Processors of Personal Data in Clouds (May 2021). URL: https://ssrn.com/abstract=4255853 (дата звернення: 29.03.2024).

32. Kamarinou, Dimitra and Millard, Christopher and Oldani, Isabella, Compliance as a Service (November 14, 2018). URL: https://ssrn.com/abstract=3284497 (дата звернення: 29.03.2023).

33. Cloud Data Processing Addendum. *Google Cloud Platform*. URL: https://console.cloud.google.com/tos?id=dpast&pli=1#dpst_customers (дата звернення: 29.03.2023).

34. What You Should Know About the EU's Cloud Code of Conduct. *4Comply*. URL: https://4comply.io/eu-cloud-code-of-conduct/ (дата звернення: 30.03.2023).

35. Christopher M. At this rate, everyone will be a [joint] controller of personal data!. *OUP Academic*. URL: https://academic.oup.com/idpl/article/9/4/217/5771498 (дата звернення: 30.03.2023).

36. Data controller or data processor | European Data Protection Board. *EDPB | European Data Protection Board*. URL: https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_en (дата звернення: 30.03.2023).

37. The Challenges of Subprocessing and Suggested Solutions under German and EU Privacy Law. Bloomberg Law News. URL: https://news.bloomberglaw.com/privacy-and-data-security/the-challenges-of-subprocessing-and-suggested-solutions-under-german-and-eu-privacy-law (дата звернення: 30.03.2023).

38. Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services. *European Data Protection Supervisor*. URL: https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html (дата звернення: 30.03.2023).

39. GDPR Update: The future of international data transfers. Deloitte Switzerland. URL: https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-the-future-of-international-data-transfer.html (дата звернення: 30.03.2023).

40. Wuermeling, Ulrich and Oldani, Isabella, Regulation of International Data Transfers in Clouds: The Impact of the GDPR (дата звернення: 30.03.2023). URL: https://ssrn.com/abstract=4255861

41. Francis M. International: Understanding data transfers under the new EU-US Data Privacy Framework. *DataGuidance*. URL: https://www.dataguidance.com/opinion/international-understanding-data-transfers-under-new (дата звернення: 30.03.2023).

42. Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows. *European Commission - European Commission*. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721 (дата звернення: 30.03.2023).

43. Everett M., Wiseman C., Singhvi A. A cautious approach: What does the EU-US adequacy decision actually mean for international data transfers?. Lexology.

URL: https://www.lexology.com/library/detail.aspx?g=a9f222c4-8154-4f30-9435-1a4c1f0f49d2 (дата звернення: 30.03.2023).

44. NIS 2 Directive. NIS 2 Directive. URL: https://www.nis-2-directive.com/ (дата звернення: 31.03.2023).

45. Difference between essential and important entities under NIS2. *ceeyu.io*. URL: https://www.ceeyu.io/resources/blog/nis-2-essential-entities-vs-important-entities-what-s-the-difference (дата звернення: 31.03.2024).

46. Will your company be subject to NIS2. ceeyu.io. URL: https://www.ceeyu.io/resources/blog/will-your-company-be-subject-to-nis2 (дата звернення: 31.03.2024).

47. NIS2 requirements. The NIS2 Directive. URL: https://nis2directive.eu/nis2-requirements/ (дата звернення: 31.03.2024).

48. Directive - 2022/2555 (NIS 2 Directive). *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022L2555 (дата звернення: 31.03.2024).

49. Walden I., Michels J. D. Getting Critical: Making Sense of the EU Cybersecurity Framework for Cloud Providers. *arXiv.org*. URL: https://arxiv.org/abs/2203.04887

50. Review of EU consumer law. European Commission. URL: https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en (дата звернення: 01.04.2024).

51. Digital fairness – fitness check on EU consumer law. *European Commission* URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en (дата звернення: 01.04.2024).

52. Call for evidence for an evaluation / fitness check : Fitness Check of EU consumer law on digital fairness від 17.05.2022 р. *European Commision.*

53. Drazewski K. EU consumer protection 2.0: Protecting fairness and consumer choice in a digital economy. *BEUC*. 2022. URL: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-

015 protecting fairness and consumer choice in a digital economy.pdf. (дата звернення: 01.04.2024).

54. Directive - 2019/770. EUR-Lex. URL: https://eur-lex.europa.eu/eli/dir/2019/770/oj (дата звернення: 01.04.2024).

55. Beale H. Digital Content Directive and rules for contracts on continuous supply. *Jipitec*. 2021. T. 12. C. 96–110. URL: https://www.jipitec.eu/issues/jipitec-12-2-2021/5286/beale_pdf.pdf (дата звернення: 01.04.2024).

56. Directive - 93/13. *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31993L0013 (дата звернення: 01.04.2024).

57. Reich N., Micklitz H.-W. The Court and Sleeping Beauty: The revival of the Unfair Contract Terms Directive (UCTD). *Common Market Law Review*. 2014. Vol. 51, Issue 3. P. 771–808. URL: https://doi.org/10.54648/cola2014061

58. Reed C., Edgar L. Consumer Protection in the Cloud. *Cloud Computing Law*. 2021. P. 218–254. URL: https://doi.org/10.1093/oso/9780198716662.003.0007

59. Directive - 2019/2161 (The Omnibus Directive). *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/dir/2019/2161/oj (дата звернення: 02.04.2024).

60. Đurović M. Adaptation of consumer law to the digital age: EU Directive 2019/2161 on modernisation and better enforcement of consumer law. *Anali Pravnog fakulteta u Beogradu*. 2020. Vol. 68, no. 2. P. 62–79. URL: https://doi.org/10.5937/analipfb2002062d (дата звернення: 02.04.2024).

61. Directive - 2020/1828 (Directive on Representative Actions). *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.409.01.0001.01.ENG (дата звернення: 02.04.2024).

62. Weißbach J. The impact of the new EU mass actions directive across Europe. *Pinsent Masons*. URL: https://www.pinsentmasons.com/out-law/guides/the-impact-of-new-eu-mass-actions-directive-across-europe (дата звернення: 02.04.2024).

63. Visscher L., Faure M. A Law and Economics Perspective on the EU Directive on Representative Actions. *Journal of Consumer Policy*. 2021. Vol. 44, no.

3. P. 455–482. URL: https://doi.org/10.1007/s10603-021-09491-3 (дата звернення: 02.04.2024).

64. Klasiček D. Inheritance Law in the Twenty-First Century: New Circumstances and Challenges. *European Union and its Neighbours in a Globalized World*. Cham, 2023. P. 235–251. URL: https://doi.org/10.1007/978-3-031-40801-4_15 (дата звернення: 03.04.2024).

65. Terletska M. The Succession Of Digital Assets In The Eu. *Tallinn Univeristy Of Tehcnology*. URL: https://www.researchgate.net/publication/365443642_THE_SUCCESSION_OF_DIGITAL_ASSETS_IN_THE_EU. (дата звернення: 03.04.2024).

66. LG Berlin, 17.12.2015 - 20 O 172/15. *dejure.org*. URL: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Berlin&Datum=17.12.2015&Aktenzeichen=20%20O%20172/15 (дата звернення: 03.04.2024).

67. Michels J. D., Millard C. Digital Assets in Clouds. *Cloud Computing Law*. 2021. P. 177–217. URL: https://doi.org/10.1093/oso/9780198716662.003.0006 (дата звернення: 03.04.2024).

68. Tar J. EU does not need to wait for the AI Act to act. *www.euractiv.com*. URL: https://www.euractiv.com/section/artificial-intelligence/opinion/eu-does-not-need-to-wait-for-the-ai-act-to-act/ (дата звернення: 03.04.2024).

69. Regulation - 2022/2065 (DSA). *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R2065 (дата звернення: 03.04.2024).

70. Digital Services Act: Questions and Answers | Shaping Europe's digital future. *European Commision*. URL: https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers

71. Europe fit for the Digital Age: new online rules for platforms. *European Commission*. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act/europe-fit-digital-age-new-online-rules-platforms_en (дата звернення: 03.04.2024).

72. Schmid D. G., Koehler P. Digital Services Act - an overview. *Lexology*. URL: https://www.lexology.com/library/detail.aspx?g=fd2c6982-8174-4b8d-860d-fb98513b6780 (дата звернення: 03.04.2024).

73. EU Digital Services Act: what will it mean for cloud services?. Hogan Lovells Engage. URL: https://www.engage.hoganlovells.com/knowledgeservices/insights-and-analysis/eu-digital-services-act-what-will-it-mean-for-cloud-services (дата звернення: 03.04.2024).

74. Manganelli A., Schnurr D. Competition And Regulation Of Cloud Computing Services: Economic Analysis And Review Of Eu Policies. *Centre on Regulation in Europe (CERRE)*, 2024. URL: https://cerre.eu/wp-content/uploads/2024/02/CERREreportCloudcomputingfeb24.p. (дата звернення: 04.04.2024).

75. Regulation - 2022/1925 (DMA). *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R1925 (дата звернення: 04.04.2024).

76. DMA designated Gatekeepers. *European Commision*. URL: https://digital-markets-act.ec.europa.eu/gatekeepers_en (дата звернення: 04.04.2024).

77. Data Act explained. *European Commision*. URL: https://digital-strategy.ec.europa.eu/en/policies/data-act-explained (дата звернення: 05.04.2024).

78. Data Act. *European Commision*. URL: https://digital-strategy.ec.europa.eu/en/policies/data-act (дата звернення: 05.04.2024).

79. Євлахова Е. Істотні умови договорів про використання технологій хмарних обчислень. *Молодий вчений*. 2021. № 11 (99). С. 19–22. URL: https://doi.org/10.32839/2304-5809/2021-11-99-4 (дата звернення: 06.04.2024).

80. Davydova N. Civil law regulation SaaS (Software as a Service) information relations. *Entrepreneurship, Economy and Law*. 2021. № 6. С. 16–22. URL: https://doi.org/10.32849/2663-5313/2021.6.03 (дата звернення: 06.04.2024).

81. Khodyko Y. Y. Legal mode of the results of works and services as civil legal objects: their unity and differentiation. *Law and Society*. 2019. Т. 3, № 1. С. 139–144. URL: https://doi.org/10.32842/2078-3736-2019-3-1-24 (дата звернення: 06.04.2024).

82. Цивільний кодекс України : Кодекс України від 16.01.2003 р. № 435-IV : станом на 8 берез. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 06.04.2024).

83. Про хмарні послуги : Закон України від 17.02.2022 р. № 2075-IX : станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 06.04.2024).

84. Klymchuk O. Cloud technologies and data centres: new regulation in Ukraine. *Sayenko Kharenko*. URL: https://sk.ua/cloud-technologies-and-data-centres-new-regulation-in-ukraine/ (дата звернення: 06.04.2024).

85. Koverznev V., Ponomarov S., Ivanov A. Legal Regulation of the Cloud Services Market of Ukraine. *European Journal of Sustainable Development*. 2024. Т. 13, № 1. С. 73. URL: https://doi.org/10.14207/ejsd.2024.v13n1p73 (дата звернення: 06.04.2024).

86. Залата О. Державні дані переміщують з України за кордон: чим це загрожує звичайним громадянам. *ФОКУС*. URL: https://focus.ua/uk/digital/519107-gosudarstvennye-danni-peremishchennya-iz-ukrajini-za-graniku-chem-eto-grozit-obychnym-grazhdanam (дата звернення: 06.04.2024)

87. Про використання банками хмарних послуг в умовах воєнного стану в Україні : Постанова Нац. банку України від 08.03.2022 р. № 42. URL: https://zakon.rada.gov.ua/laws/show/v0042500-22#Text (дата звернення: 06.04.2024).

88. Деякі питання забезпечення функціонування державних інформаційних ресурсів : Постанова Каб. Міністрів України від 30.12.2022 р. № 1500. URL: https://zakon.rada.gov.ua/laws/show/1500-2022-п#Text (дата звернення: 06.04.2024).

89. Про внесення змін до деяких законів України щодо удосконалення порядку обробки та використання даних у державних реєстрах для військового обліку та набуття статусу ветерана війни під час дії воєнного стану : Закон України від 16.01.2024 р. № 3549-IX. URL: https://zakon.rada.gov.ua/laws/show/3549-20#Text (дата звернення: 06.04.2024).

90. Interfax-Ukraine. How the Consumption of Cloud Services Has Changed. GigaCloud Report 2022. *Interfax-Ukraine*. URL: https://en.interfax.com.ua/news/blog/888920.html (дата звернення: 07.04.2024).

91. Про використання у період дії воєнного стану учасниками фондового ринку хмарних послуг та/або послуг центру обробки даних : Рішення Нац. комісії з цін. паперів та фонд. ринку від 04.08.2022 р. № 1054. URL: https://zakon.rada.gov.ua/rada/show/v1054863-22 (дата звернення: 07.04.2024).

92. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 07.04.2024).

93. Yevlakhova E. R. General theoretical principles of protection of the rights and interests of the subjects of contractual relations in the field of cloud computing technologies. *Juris Europensis Scientia*. 2023. № 1. С. 33–41. URL: https://doi.org/10.32782/chern.v1.2023.6 (дата звернення: 07.04.2024).

94. Кодекс України про адміністративні правопорушення (статті 1 - 212-24) : Кодекс України від 07.12.1984 р. № 8073-X : станом на 14 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 07.04.2024).

95. Задніпровська О. Цивільні позови в Україні про захист персональних даних. *Medium*. URL: https://medium.com/axonpartners/цивільні-позови-в-україні-про-захист-персональних-даних-ba0cc67a5980 (дата звернення: 07.04.2024).

96. Проект Закону про захист персональних даних №8153 від 25.10.2022. *Офіційний вебпортал парламенту України*. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (дата звернення: 07.04.2024).

97. Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації № 6177 від 18.10.2021.

Офіційний вебпортал парламенту України. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/27996 (дата звернення: 07.04.2024).

98. Про цифровий контент та цифрові послуги : Закон України від 10.08.2023 р. № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text (дата звернення: 07.04.2024).

99. The Latest Cloud Computing Statistics (updated March 2023). *AAG*. URL: https://aag-it.com/the-latest-cloud-computing-statistics/ (дата звернення: 29.02.2024)

100. Barroca J. G., Buxo A. Cloud sovereignty: Three imperatives for the European public sector. *Deloitte*. URL: https://www2.deloitte.com/xe/en/insights/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html. (дата звернення: 29.02.2024)

101. Музика Л. А. Концепція цивільно-правової політики України : монографія / Л. А. Музика ; Національний університет "Києво-Могилянська академія". - Київ : Паливода А. В., 2020. - 503 с. URL: https://ek-mair.ukma.edu.ua/handle/123456789/21911 (дата звернення: 29.02.2024)