EULIoT

National Technical University
of Ukraine "Igor Sikorsky
Kyiv Polytechnic Institute"

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет соціології і права

О. Баранов, О. Головко, М. Дубняк

ГАРМОНІЗАЦІЯ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА ДО ЄВРОПЕЙСЬКИХ ПРАКТИК У СФЕРІ ІНТЕРНЕТУ РЕЧЕЙ

МОНОГРАФІЯ

КИЇВ-ОДЕСА
ФЕНІКС
2023

УДК 004.738:340.113(477)+061.1ЄС
Г 20

Автори:

Баранов Олександр – доктор юридичних наук, професор, керівник Наукового центру цифрової трансформації і права Державної наукової установи «Інститут інформації, безпеки і права» Національної академії правових наук України». Академічний лідер проєкту «Європейська інтеграція: законодавство та Інтернет речей».

Головко Ольга – кандидат юридичних наук, старший дослідник, старший викладач кафедри інтелектуальної власності та приватного права КПІ ім. Ігоря Сікорського. Координатор проєкту «Європейська інтеграція: законодавство та Інтернет речей».

Дубняк Марія – кандидат юридичних наук, старший викладач кафедри інформаційного, господарського та адміністративного права КПІ ім. Ігоря Сікорського. Менеджер проекту «Європейська інтеграція: законодавство та Інтернет речей».

Баранов О., Головко О., Дубняк М.

Г 20 Гармонізація національного законодавства до європейських практик у сфері Інтернету речей : монографія / О. Баранов, О. Головко, М. Дубняк ; КПІ ім. Ігоря Сікорського. – Київ; Одеса : Фенікс, 2023. – 108 с.

ISBN 978-617-8395-04-9

У монографії досліджуються питання гармонізації норм Регламентів і Директив ЄС для розбудови технологій Інтернету речей в Україні.

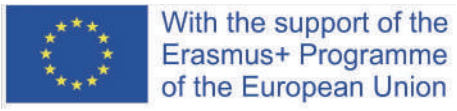
Рекомендується науковцям, державним службовцям, підприємцям, правникам, викладачам, студентам та аспірантам, а також усім, хто цікавиться проблемами правового регулювання суспільних відносин у сфері застосування штучного інтелекту, робототехніки, криптовалют, технологій блокчейн, хмарних технологій, великих даних та інших складових Інтернету речей (IoT), правовим забезпеченням цифрової трансформації, дослідженням національного законодавства та законодавства Європейського Союзу з питань забезпечення кібербезпеки, вільного обігу даних, захисту персональних даних.

УДК 004.738:340.113(477)+061.1ЄС

ISBN 978-617-8395-04-9

Матеріали подано в авторській редакції.

Написання та публікація монографії здійснені в рамках реалізації міжнародного проєкту у сфері освіти «Європейська інтеграція: законодавство та Інтернет речей» у рамках напряму Жан Моне «Модуль» програми «Erasmus+» № 620017-EPP-1-2020-1-UA- EPPJMO-MODULE (спільний проєкт КПІ ім. Ігоря Сікорського, Еразмус+ Жан Моне Фонду та Виконавчого агентства з питань освіти, аудіовізуальної діяльності та культури за підтримки ЄС).



Зміст

ВСТУП

У монографії визначено актуальні та ключові аспекти найважливіших сегментів гармонізації норм Регламентів та Директив ЄС для розбудови технологій Інтернету Речей в Україні, з метою запозичення кращих практик правового регулювання, які відповідають актуальним цілям євроінтеграції. Ця публікація стане вагомим внеском у розвиток досліджень євроінтеграційних процесів у сфері IoT.

Методологія. Автори дотримуватимуться принципів максимального використання особливостей нормопроектування як національної правової системи, так і системи європейського законодавства з урахуванням стану та перспектив впровадження новітніх цифрових технологій, концептуальних засад їх розвитку.

Робота базується на сучасних науково-правових дослідженнях вчених різних країн та рівнів наукової експертизи, зокрема, на результатах різних дослідницьких груп, створених Європейською Комісією у сфері впровадження IoT.

Розділ І

ІНТЕРНЕТ РЕЧЕЙ ТА ТЕХНОЛОГІЇ БЛОКЧЕЙН

Інтернет речей та горизонтальні бізнес-відносини
Технологічні можливості забезпечення довіри
Забезпечення довіри через використання технологій блокчейн
Складові елементи технології блокчейн
4 етапи інноваційного використання блокчейну
Правові проблеми застосування технології блокчейн

Інтернет речей та горизонтальні бізнес-відносини

Практично з самого початку масового використання Інтернет-технологій виникли проблеми, пов'язані з особливостями мережі Інтернет: потенційна анонімність суб'єктів відносин, невизначеність їх юрисдикції, часу здійснення транзакцій і достовірності отриманої інформації та ряд інших [1]. Для нейтралізації негативних наслідків прояву цих особливостей як національні правові системи, так і міжнародне право відреагували появою певних нормативно-правових актів з метою забезпечення довіри в процесі здійснення різних транзакцій, заснованих на використанні Інтернет-технологій.

Вирішенню проблем довіри до Інтернету як до відкритого середовища присвячено ряд міжнародних документів: Доповідь Генерального секретаря ООН [2], аналітичний огляд ISOC "Рамки політики для відкритого і надійного Інтернету" [3], Глобальний звіт ISOC "Економіка побудови довіри в Інтернеті: запобігання спотворенню даних" [4] і багато інших. Квінтесенція цих підходів полягає в наступній думці: Інтернет потребує надійного фундаменту довіри, щоб повністю реалізувати його потенціал [3].

В якості одного з інструментів підвищення довіри між суб'єктами, що здійснюють транзакції за допомогою мережі Інтернет, особливо, в умовах зростаючої кількості видів і типів кіберзагроз, пропонується використовувати технології блокчейн [5-8].

Цілком очевидно, що більшість проблем, які мають місце при використанні інтернет-технологій, будуть мати місце і у сфері Інтернету речей (IP), в якій мережа Інтернет є базовою інфраструктурною платформою.

З урахуванням економічної привабливості, передбачуваної безпрецедентності масового використання технологій IP, проблема забезпечення довіри буде набувати все більш важливого значення.

Таким чином, дослідження в сфері IP правових методів і механізмів забезпечення довіри, зокрема, з використанням для цього технологій блокчейн, має значну актуальність.

На основі результатів роботи [9], а також проведеного аналізу юридичних і технічних джерел запропонуємо в інтересах цього дослідження наступне визначення: ***Інтернет речей*** *– це сукупність взаємодіючих технічних систем і комплексів, що складаються з мікропроцесорів, сенсорів, пристроїв, систем передачі даних, локальних і/або розподілених обчислювальних ресурсів і програмних засобів, в тому числі програм штучного інтелекту, на основі використання величезної кількості даних і мережі Інтернет та призначених для реалізації суспільних відносин, зокрема, пов'язаних з наданням послуг або проведенням робіт за безпосередньою участю або без участі суб'єктів цих відносин (юридичних або фізичних осіб*).

Спираючись на базове для інституційної економіки поняття економічної транзакції [10], сформулюємо таке поняття: ***транзакція*** *– це добровільна взаємодія (спільна дія в інтересах один одного), що здійснюється за згодою суб'єктів щодо ресурсів або дій (предмета транзакції).*

Можна припустити, що феномен IP, його величезні економічні, соціальні та технологічні переваги будуть причиною істотної зміни ландшафту бізнес-моделей в сучасному і майбутньому світі – світі технологій IP.

Сучасні бізнес-моделі взаємодії різних суб'єктів містять елементи ієрархічних зв'язків, які, як правило, обумовлені необхідністю взаємодії з суб'єктами публічної влади. Ця необхідність зумовлена існуючими національними та міжнародними системами сертифікації, ліцензування, квотування, фітосанітарного контролю та переміщення вантажів, платіжними та митними системами тощо. Наявність ієрархічних зв'язків призводить до збільшення непродуктивних транзакційних витрат ведення бізнесу, які значно збільшуються для компаній, розташованих в різних

країнах. Так, наприклад, сьогодні реальний час необхідний для здійснення власне угоди купівлі-продажу нерухомого або рухомого майна вже може обчислюватися хвилинами, але підготовка необхідних документів для переоформлення права власності може зайняти кілька днів.

Так як причина збільшення транзакційних витрат (далі – ТВ) – це наявність ієрархічних зв'язків з державними органами, то, природньо, напрошується радикальне рішення: шлях мінімізації ТВ – це шлях усунення ієрархічних зв'язків. Або, іншими словами, це означає міграцію від ієрархічної структури бізнес відносин до горизонтальної (плоскої) структури. ***Горизонтальні бізнес-відносини*** – це пірингові відносини (peer to peer), тобто однорангові відносини між рівними партнерами без посередників.

В останні роки завдяки використанню мережі Інтернет відносини між різними суб'єктами як національної, так і іноземної юрисдикції активно реалізуються відповідно до горизонтальної моделі взаємодії. Безсумнівно, це повною мірою стосується і випадків використання технологій Інтернету речей. Яскравим прикладом можливостей IP для реалізації піринговых відносин між виробником і споживачем можуть бути відносини, що пов'язані з технологіями 3D-друку. Зростаюча сфера застосування 3D- друку та простота його використання дозволяють припустити, що в майбутньому стане можливою організація масового "виробництва" товарів на дому у споживачів відповідно до їх індивідуальних замовлень. Така "поставка" товарів не потребуватиме ані торгових посередників, ані ієрархічних зв'язків.

Відзначимо кілька системних факторів розвитку світової економіки, які стимулюють перехід до горизонтальних бізнес-моделей:

Ц глобалізація економічних, виробничих, інформаційних, фінансових та інших відносин;

Ц зростання конкуренції як на національному, так і на міжнародному рівні;

Ц зростання міжнародної конкуренції, тобто конкуренції на національних локальних ринках окремих країн гравців локальних ринків з інших країн світу;

Ц наявність міцного кореляційного зв'язку результатів ведення бізнесу та невизначеності і волатильності попиту на продукцію або послуги;

Ц необхідність для гравців локальних ринків швидкого освоєння знань про особливості конкретних юрисдикцій не тільки в цілому інших держав, але навіть їх окремих регіонів;

Ц прискорення темпів протікання і розвитку всіх процесів в соціумі, і, перш за все, в економіці;

Ц необхідність різкого збільшення швидкості та підвищення якості реакції на виклики.

Таким чином, формування горизонтальних бізнес-відносин на основі Інтернет- технологій створює унікальні передумови для надання послуг і проведення робіт в інтересах суб'єктів (фізичних або юридичних осіб) з мінімальними, іноді, навіть, з нульовими, транзакційними витратами завдяки усуненню ієрархічних зв'язків.

Однак, має місце фундаментальний фактор, який стримує перехід до горизонтальних моделям взаємовідносин – це довіра, вірніше, її відсутність.

Технологічні можливості забезпечення довіри

Словники в основному однаково тлумачать довіру, наприклад, як переконаність в чесності, порядності; віра в щирість і сумлінність будь-кого [11].

Розуміння людством значення фактору довіри в економічній практиці виникає досить давно. Імовірно, з того часу, коли в торгові взаємовідносини стали масово залучатися суб'єкти з невідомою один для одного репутацією, що створювало цілком відчутний

фактор ризику реалізації загроз, пов'язаних з недобросовісною поведінкою суб'єкта транзакцій. Заходи, які необхідно було проводити для мінімізації цього ризику, збільшували ТВ, але інакше була реальна ймовірність отримати набагато більші ТВ в разі реалізації загроз.

Таким чином, однією з причин збільшення ТВ була недобросовісна поведінка суб'єктів транзакції [10], яку не можна було заздалегідь виключити через відсутність підстав для безумовної довіри до них.

У даній роботі будуть досліджуватися проблеми мінімізації тільки тих ТВ, наявність яких обумовлено фактором відсутності довіри.

Проблема довіри загострюється тоді, коли в якості еквівалента товару стали масово використовуватися національні "гроші", специфічні для кожного державного (квазідержавного) утворення. Наявність різних еквівалентів створювало ризики при здійсненні транзакцій, що вимагало формування довірчих механізмів обміну цими еквівалентами. Функцію забезпечення довіри при обміні еквівалентів стали виконувати треті особи – посередники при обміні національних "валют" (міняйли), які обслуговували будь-якого учасника ринку. Природно, за свою послугу міняйли стягували певну плату, що і становило частину ТВ, обумовлених наявністю ієрархічного зв'язку між покупцями (продавцями) і такою інституцією як міняйли.

Назвемо таку систему обміну національними "валютами" – централізованою системою довіри. ***Централізована система довіри*** (далі – ЦСД) – це система, в якій носієм довіри (інформації про довіру) до суб'єктів взаємовідносин є спеціальний центральний (єдиний, загальний) елемент системи, що функціонує в інтересах будь- якого і кожного суб'єкта соціуму. ***Інформація про довіру*** – це достовірна, повна і своєчасна інформація про сумлінному (несумлінному) поведінку суб'єкта.

У своїй статті М. Зейдель вводить поняття розподіленої форми довіри – це коли люди, раніше невідомі один одному, можуть вступати в безпосередні, рівні довірливі стосунки без звернення до якоїсь центральної організації, яка ручається за будь-якого з них [12]. Цілком можна погодитися з таким підходом визначення особливостей довіри у відсутності ЦСД, але слід зауважити, що така форма довіри може охоплювати не тільки тих, хто раніше був невідомий один одному, але також і тих, хто знав один одного раніше. При цьому, необхідно пам'ятати, що така розподілена система довіри створюється на засадах самоорганізації та добровільного приєднання до неї. Для розподіленої системи довіри можуть бути створені і використані різні механізми забезпечення довіри.

Отже, ***розподілена система довіри*** (далі – РСД) **–** це особливого роду організаційна система, формально чи не формально створена як закрита корпорація, в якій носієм довіри (інформації про довіру) до суб'єктів взаємовідносин є будь-який суб'єкт, але який обов'язково входить до цієї корпорації.

Аналіз функціонування РСД дозволяє виділити основні властивості притаманні саме цій формі довіри:

Ц зберігання інформації про довіру здійснюється кожним суб'єктом незалежно від інших;

Ц інформація про довіру не зберігається в централізованому місці (бібліотеці, журналі, реєстрі, базі даних), а зберігається розподілено – кожним суб'єктом;

Ц вільний доступ або обмін інформацією про довіру до будь-якого суб'єкта для всіх членів РСД;

Ц розголос виявлених фактів порушення довіри або прояви якимось суб'єктом нечесності, непорядності або несумлінності.

Отже, ми приходимо до розуміння того, що проблема довіри – це проблема створення та функціонування деякої інформаційної системи (централізованої або розподіленої), яка забезпечує збір, накопичення, використання і зберігання достовірної, повної та

своєчасної інформації про сумлінну (несумлінну) поведінку суб'єктів взаємовідносин. Тому, завдання створення правових механізмів вирішення проблеми довіри відноситься до завдань інформаційного права.

Таким чином, будемо розуміти ***довіру*** – як наявність своєчасної, повної та достовірної інформації про сумлінну поведінку.

Для майбутнього використання технологій IP завдяки ряду переваг кращими є горизонтальні бізнес відносини, які в свою чергу можуть гуртуватися на стійких або нестійких горизонтальних транзакційних зв'язках.

До типових стійких горизонтальних транзакційних зв'язків можна віднести, наприклад, зв'язки між членами замкнутих професійних корпорацій. Саме наявність корпоративної довіри дозволяє такі стійкі горизонтальні транзакційні зв'язки вважати довірчими. До стійких горизонтальних транзакційних зв'язків умовно можна також віднести зв'язки, що складаються відповідно до договору, укладеного в результаті тривалих переговорів, або багаторазово повторювані зв'язки між одними і тими ж суб'єктами, що власне і формує якусь неформальну квазікорпорацію. Такі стійкі зв'язки супроводжуються накопиченням достовірної та повної інформації про сумлінну (несумлінну) поведінку суб'єктів корпорації. Отже, стійкі горизонтальні транзакційні зв'язки мають високий ступінь довіри, що дозволяє звести до нуля транзакційні витрати усередині корпорації, а іноді і за її межами.

Таким чином, можна дати наступне визначення**: *стійкі горизонтальні транзакційні зв'язки*** – це багаторазово повторювані взаємовідносини між відомими один одному суб'єктами з приводу однорідних транзакцій. Однорідність транзакцій означає високу ступінь подібності умов здійснення взаємовідносин, а значить передбачає стабільність (сумлінної чи несумлінної) поведінки суб'єктів.

Антиподом розглянутим зв'язкам є ***нестійкі горизонтальні транзакційні зв'язки*** як разові або нечисленні спорадичні взаємовідносини між відомими або невідомими один одному суб'єктами, які виникають завдяки попиту або потребам, що ситуативно виникли. Спорадичність і нечисленність взаємовідносин не сприяють накопиченню достовірної та повної інформації про сумлінну (несумлінну) поведінку суб'єктів цих відносин. Спорадичні взаємовідносини, як правило, характерні для відкритих систем, тобто систем, відкритих для взаємодії між будь-якими суб'єктами. До таких систем, в першу чергу, можуть бути віднесені ті, які функціонують на базі використання Інтернет- технологій. Це в повною мірою стосується і Інтернету речей.

Отже, в умовах використання технологій IP будуть мати місце переважно нестійкі горизонтальні транзакційні зв'язки, що особливо гостро ставить питання забезпечення довіри.

Традиційно проблема забезпечення довіри вирішувалася шляхом створення деякої третьої сторони – централізованої спеціальної інституції, апріорі такою, що заслуговує на довіру (credible institution), в якій у той чи інший спосіб збиралася інформація про довіру (благонадійність) до можливих суб'єктів суспільних відносин. До недавнього часу вважалося, що централізовані організаційні структури є найкращим способом вирішення проблеми довіри. У разі законодавчого регулювання функціонування централізованої системи довіри, така система може бути використана будь-яким членом соціуму. Як приклад можуть служити банківська система, система нотаріату, офіційні реєстри нерухомого майна чи земельних ділянок, система сертифікації електронно-цифрових підписів тощо. Безсумнівно, необхідність правового регулювання відносин, пов'язаних з ЦСД, і необхідність фінансування її діяльності зумовлює збільшення прямих і непрямих ТВ.

Виходячи з вищесказаного, можемо констатувати наявність для ЦСД наступного протиріччя:

Ц з одного боку, довіра є необхідною умовою зменшення ТВ;

Ц з іншого – збільшення ТВ є необхідною умовою для забезпечення довіри (зменшення ступеня ризику) при здійсненні нестійких горизонтальних транзакційних зв'язків.

На думку М. Зейделя, раніше вважалося, що саме організаційні структури забезпечують централізоване джерело легітимності і це є основою розвитку організаційної екології, інституціональної теорії і економічної теорії транзакційних витрат [12]. Іншими словами, це означало, що довіру може бути забезпечено тільки за рахунок введення ЦСД.

Однак, інтерпретація відомої теореми нобелівського лауреата 1991 року з економіки Р. Коуза, говорить про те, що тільки наявність транзакційних витрат у відносинах між економічними агентами призводить до необхідності введення зовнішнього регулювання і, власне, призводить до необхідності появи третіх осіб або іншими словами, до появи спеціалізованих організаційних структур [13; 14]. Але, якщо сформулювати зворотну теорему, то вона зведеться до наступного: мінімізація ТВ економічних агентів при їх взаємодії, що в ідеалі прагнуть до нуля, нівелює роль зовнішнього регулювання, а значить виключає необхідність в створенні якихось спеціалізованих організаційних структур.

У свою чергу, зворотна теорема дозволяє сформулювати гіпотезу про те, що якщо якась система відносин між економічними агентами має нульову вартість транзакцій, то така система не потребує наявності якоїсь централізованої організації для аутентифікації сторін угод і підтвердження довіри.

Іншими словами, приходимо до важливого висновку про те, що система відносин між економічними агентами, в якій є інформація про довіру до кожного, – це система з нульовою вартістю транзакцій.

Одним з факторів, що формує вимоги до систем довіри як до інформаційних систем, є часовий чинник. Транзакції, які здійснюються за допомогою Інтернет- технологій, мають істотні

переваги перед іншими способами їх здійснення завдяки високій швидкості їх реалізації. Отже, будь-яка система довіри потенційно повинна мати швидкодію (час) реакції менше часу, необхідного на реалізацію транзакції. В іншому випадку система довіри буде причиною збільшення ТВ. Особливо негативно це може позначитися на каскадних бізнес-процесах, що складаються з великої кількості високоінтегрованих складно організованих горизонтальних транзакційних зв'язків, що як раз і є характерним для технологій IP.

Крім того, проблема забезпечення довіри в останні роки значно загострилася через стрімко прогресуючі методи та засоби реалізації кіберзагроз.

Для бізнес-моделей, що реалізуються в умовах використання технологій IP, найбільш поширеними і масовими будуть нестійкі (випадкові) горизонтальні транзакційні зв'язку, в яких:

Ц суб'єкти можуть здійснювати транзакції з різних місць і в різний час;

Ц час отримання об'єктів транзакцій (товарів, послуг, платіжних засобів тощо) для суб'єктів може бути різним;

Ц суб'єкти можуть не знати не тільки один одного, але й не знати нічого один про одного;

Ц репутація суб'єктів, в традиційному її розумінні, практично нічого не означає в умовах, коли тимчасові і вартісні витрати на її перевірку істотно збільшують транзакційні витрати в порівнянні з вартістю угоди.

Отже, фактор довіри, тобто методи і способи збору, зберігання і обробки інформації про довіру до суб'єктів транзакцій при використанні технологій IP в умовах формування нестійких горизонтальних бізнес-моделей набуває фундаментальне значення.

Тому тільки динамічна в функціонуванні, максимально економічна для суб'єктів транзакцій, доступна розподілена інформаційна система, що має своєчасну, повну і достовірну

інформацію про довіру, може створити умови для реалізації всіх переваг технологій ІР.

Все йде до необхідності відновлення в умовах розвитку технологій Інтернету історично раніше широко розповсюдженого способу здійснення транзакцій – "вдарили по руках" (handshake), коли суб'єкти без складання письмового договору простим рукостисканням здійснювали транзакції на багато мільйонів з практично нульовими ТВ. Настільки велика була сила репутації і довіри. Звичайно, відновлення способу "вдарили по руках" має буде здійснюватися на нових організаційних і технологічних принципах і рішеннях.

Таким чином, одним з можливих варіантів розв'язання проблеми довіри в умовах використання технологій ІР є створення РСД, що потребує широких досліджень в різних галузях знань, в тому числі, і в такій галузі як інформаційне право. Тому дослідження правових проблем, наприклад, пов'язаних з визначенням правових принципів побудови і функціонування РСД як інформаційної системи, визначення правових механізмів збору, використання і зберігання інформації про довіру, взаємодії РСД з іншими системами довіри і розгляду ймовірних спорів є дуже актуальними саме на порозі широкого впровадження технологій ІР.

Забезпечення довіри через використання технологій блокчейн

Р. Меллон вважає, що технології блокчейн усувають необхідність в звичних економічних, правових і політичних інститутах, які в традиційній економіці виконують роль посередників довіри, оскільки усувають власне необхідність довіри, замінюючи її доказами [15].

На Світовому економічному форумі в Давосі (2015 р.) було дано таке визначення: блокчейн – нова технологія, яка усуває

необхідність третіх осіб для забезпечення довіри до фінансових, договірних та виборних дій [16].

Існують інші, більш технократичні визначення, наприклад: блокчейн – це послідовна база даних інформації, яка захищена методами криптографічного доказу і пропонує альтернативу класичним фінансовим книгам [17]. Або, блокчейн – публічна база всіх здійснених транзакцій різного типу в рамках єдиної системи, які шикуються певним чином і з них формується ланцюжок блоків.

На думку експертів, блокчейн буде застосовуватися в найрізноманітніших сферах, таких як: грошові перекази, мікроплатежі, розумні контракти (або смарт-контракти), ідентифікація фізичних об'єктів і активів, державне управління, оборона і безпека, міжнародна діяльність тощо. В цілому, передбачається, що в майбутньому технології блокчейн можуть стати драйвером радикальних змін в широкому спектрі галузей, бізнес-моделей, соціальних і операційних процесів [17]. Тестування та впровадження технологій блокчейн розпочали в ряді країн і у багатьох великих корпораціях.

З одного боку, багато дослідників слідом за Д. Тапскоттом [18] підносять трансформаційний потенціал технологій блокчейн не тільки в бізнесі, але в багатьох інших сферах: політичній, державного управління, попередження корупції, освіті та культурі, захисту прав громадян тощо. З іншого боку, існує досить ґрунтовний скепсис щодо можливостей і перспектив використання технологій блокчейн. Цілком очевидно, що крапку над "і" розставить історичний досвід і результати практичного використання цих технологій в різних додатках. Важливу роль в успіху цього досвіду буде відігравати наявність відповідного правового регулювання там, де це буде необхідно, що заздалегідь нівелює можливість виникнення юридичних бар'єрів на шляху використання можливостей технологій блокчейн.

З урахуванням того, що технологія блокчейн реалізується за допомогою комп'ютерних і програмних засобів, а функціонує на

базі використання мережі Інтернет, то для нейтралізації можливих атак хакерів або недобросовісних дій з інформацією використовуються криптографічні засоби.

У технологічному сенсі блокчейн – однорангова комп'ютерна мережа, яка функціонує поверх мережі Інтернет, була представлена в жовтні 2008 року в рамках пропозиції щодо біткойну (віртуальної валютної системи), яка не потребувала централізованого управління емісією, юридичної передачі права власності та підтвердження транзакцій [19].

Дуже цікаве і реалістичне обґрунтування появи технологій блокчейн, що практично збігається з викладеним вище баченням про необхідність побудови РСД, викладено в роботі [20]. Автори вважають, що системи розрахунків в сучасній економіці базуються на ієрархічних кореспондентських відносинах банків з величезним числом посередників (в тому числі і на валютному ринку), що обумовлює:

Ц імітування інформаційного он-лайну за рахунок досить великого ланцюжка посередників, які страхують ризики один одного;

Ц високу вартість проведення платежів;

Ц ризики, пов'язані з поняттям операційного дня і можливими різними датами виконання платежів;

Ц ризики невиконання або оспорювання сторонами угоди проведених платежів;

Ц додаткової ліквідності для платіжних систем.

Нейтралізація всіх цих недоліків традиційними методами призводить до необхідності створення кваліфікованого фінансового посередника (довіреної третьої сторони: клірингові системи, депозитарії, системи передачі фінансової інформації типу Reuters або SWIFT). Однак, використання посередників призводить до чергового значного подорожчання і уповільнення розрахунків (міжнародні фінансові транзакції – до семи днів).

Таким чином, в банківській сфері констатуються серйозні протиріччя між сформованим традиційним бізнесом і сучасними інноваційними технологіями.

Вихід з цієї ситуації знайшли у використанні технології блокчейн, яка за визначенням не вимагає третіх осіб для реалізації функції посередника, що підтверджує інформацію про довіру до суб'єкта.

Складові елементи технології блокчейн

Наведемо опис технології блокчейна з цікавої праці [20]. Блокчейн – це мережа, що складається з елементів (комп'ютери/суб'єкти), які називаються вузлом, кожен з яких містить (зберігає) ланцюжок блоків (книгу). Кожен блок містить набір транзакцій, здійснених з моменту закінчення формування попереднього блоку мережі до моменту складання цього блоку, розмір якого залежить від того, скільки транзакцій було завершено в заданий інтервал часу. Повідомлення про транзакції включає відомості про публічну адресу одержувача, вартості транзакції і криптографічного цифрового підпису, який доводить справжність транзакції. Вузли мережі, отримавши повідомлення від будь- якого іншого вузла, підтверджують справжність і дійсність повідомлення шляхом дешифрування цифрового підпису. Різні мережі блокчейнів використовують різні методи прийняття рішення про сумлінність транзакції і відсутність шахрайства. Новий блок одним з вузлів в мережі поміщається в оновлену версію книги (реєстру, бази даних), в якій містяться всі попередні блоки. Всі блоки блокчейна криптографічним методом пов'язані один з одним таким чином, що зробити зміни в будь-який з них неможливо.

Технології блокчейн мають наступні основні властивості в рамках певної мережі блокчейн, що об'єднує деяку обмежену сукупність суб'єктів:

Ц можливість зберігання інформації для кожної транзакції суб'єкта у вигляді незалежних записів;

Ц можливість зберігати для кожної транзакції різноманітну інформацію, наприклад, про права власності, звіти по кредитуванню, якість товарів і так далі;

Ц реєстр транзакцій не зберігається в певному місці, а розподіляється на тисячі комп'ютерів (суб'єктів) по всьому світу;

Ц наявність вільного доступу у суб'єктів до всього реєстру (книги) транзакцій.

Таким чином, блокчейн є публічною базою даних всіх транзакцій між суб'єктами мережі блокчейн. Оскільки мережа блокчейна відкрита для вільного приєднання, то публічність даних мережі фактично означає загальнодоступність цих даних.

Що дає технологія блокчейна людству? На думку авторів фундаментальної роботи [18], вперше в історії дві сторони, які не знають і не довіряють одна одній, можуть безпосередньо вести бізнес та інші будь-які справи, оскільки перевірка особистості та встановлення довіри більше не є правом і привілеєм фінансового посередника. Більш того, в контексті фінансових послуг протокол довіри приймає подвійне значення. Блокчейн також може встановлювати довіру, перевіряючи особистість і потенціал будь-якого контрагента за допомогою комбінації минулої історії транзакцій (за блочним ланцюжком), показників репутації на основі узагальнених оглядів та інших соціально-економічних показників.

4 етапи інноваційного використання блокчейну

Спираючись на результати досліджень [21], наведемо порівняльні характеристики 4-х фаз інноваційного розвитку використання (додатків) мережі Інтернет та блокчейна.

1. Одиничне застосування – додатки з невисокою новизною (електронна пошта і біткойн). Фактично це реалізація відомих

інформаційних технологій на новій технологічній базі. Практична відсутність необхідності в координації.

2. Локалізація – додатки містять відносну новизну, розроблені в інтересах обмеженої кількості користувачів (електронний документообіг та облік поставок). Фактично це реалізація окремих етапів бізнес процесів на новій технологічній базі. Невисокі вимоги до рівня координації.

3. Заміщення – це суперпозиція двох перших фаз (одиничного і локалізованого застосування) і має відповідну технологічну новизну в інтересах необмеженої кількості користувачів (електронна торгівля і криптовалютні системи). Фактично це реалізація нових або модернізація бізнес процесів завдяки використанню нових технологій. Вимагає високого рівня координації, оскільки може охоплювати велику кількість галузей і сфер діяльності.

4. Трансформація – це абсолютно нові додатки, які мають потенціал для змін природи економічних, соціальних і політичних відносин (Інтернет речей і smart- контракти). Фактично це реалізація нових методів і способів системного ведення бізнесу, що повністю базуються на використанні нових технологій. Вимагає не тільки високого рівня координації, а й інституційної угоди щодо стандартів і процесів в економічній, соціальній, правовій та політичних сферах.

Передбачається, що один з основних технологічних бар'єрів поширення технологій блокчейн – це труднощі при масштабуванні блоку, пов'язані з тим, що кожен комп'ютер в мережі обробляє кожну транзакцію, буде подолано в найближчому майбутньому і це відкриє перспективи для використання технологій блокчейн в Інтернеті речей [22].

Правові проблеми застосування технології блокчейн

Що стосується юридичних бар'єрів, то в частині вирішення проблеми формування правового забезпечення широкого застосування технологій блокчейн з урахуванням результатів, отриманих в роботі [23] можна сформувати наступні завдання, що стоять перед правовою наукою, зокрема, перед інформаційним правом:

1. Систему правового регулювання застосування технологій блокчейн доцільно розробляти в парадигмі максимальної інтеграції в традиційну національну правову систему.

2. Для низки публічних додатків технологій блокчейн задля зниження ризиків необхідно визначення юридичного статусу мережі блокчейн, її реєстру і записів транзакцій, формування правових вимог до їх форми і змісту.

3. Визначення юрисдикції реєстру мережі блокчейн, в тому числі, при наявності транскордонних транзакцій.

4. Дослідження особливостей правовідносин, пов'язаних з технологіями блокчейн, юридичних прав, обов'язків і відповідальності сторін.

5. Дослідження проблеми визначення юридичних ризиків та обмежень використання технологій блокчейн в різних сферах застосування.

6. Формування правових механізмів нагляду, встановлення відповідальності за порушення прав суб'єктів мережі блокчейн і відшкодування завданих збитків або при наявності помилок в комп'ютерній програмі.

1. Вирішення правовими засобами проблеми наявності неповної спостережливості з боку суб'єктів мережі блокчейн всіх прихованих дій програмного забезпечення, що реалізує ту чи іншу функцію технології блокчейн, що може привести до небажаного збитку.

2. Розробка правових механізмів верифікації суб'єктів мережі блокчейн (в разі необхідності), які здійснюють транзакцію, на момент її здійснення.

3. Вирішення протиріччя між законодавчими вимогами обмеження доступу до персональних даних та іншої чутливої інформації суб'єктів мережі блокчейн, яка може міститися в реєстрі цієї мережі, і відкритістю інформації для всіх суб'єктів по всіх транзакціях та їх зберіганням в кожному вузлі мережі блокчейн.

4. Установити правову регламентацію забезпечення, перевірки і сертифікації (при необхідності) кібербезпеки як програмного забезпечення, що підтримує функціонування мережі блокчейн, так і програмно-апаратних платформ, на яких розміщується це програмне забезпечення.

5. Розробка пропозицій щодо процесуальних особливостей розгляду у суді суперечок, пов'язаних з мережами блокчейн.

Висновки

1. У всьому світі розвиток технологій ІР буде пов'язано з стрімким зростанням кількості нестійких горизонтальних транзакційних зв'язків, які вимагатимуть системи довіри до суб'єктів взаємовідносин.

2. Найбільш економічними, що мінімізують транзакційні витрати і забезпечують суб'єктів взаємовідносин своєчасною, повною та достовірною інформацією є розподілені системи довіри.

3. В даний час технології блокчейн формують найкращі технологічні умови побудови розподілених систем довіри для суб'єктів, що вступають в нестійкі горизонтальні транзакційні зв'язки в сфері ІР.

4. Використання в майбутньому технологій блокчейн вимагатимє міждисциплінарних досліджень як власне розвитку та особливостей застосування цих технологій для різних додатків, так і спеціальних питань, пов'язаних з визначенням стратегій і соціальних

наслідків їх застосування, цілісністю і повнотою даних, захистом приватності, конфіденційністю, кібербезпекою і багато інших, в тому числі, і досліджень правових проблем.

5. У сфері права застосування як технологій IP, так і технологій блокчейн в публічних або загальносуспільних сферах неминуче спричинить необхідність досліджень, як мінімум, питань встановлення та розподілу юридичної відповідальності у разі настання небажаних наслідків або визначення правових умов недопущення або відновлення порушених прав учасників відповідних суспільних відносин, а також багатьох інших, які неминуче виникнуть при використанні публічних і приватних мереж блокчейн.

6. Найкращою стратегією майбутніх правових досліджень було б орієнтування на створення таких правових конструкцій, які б максимально інтегрувалися в традиційну національну і міжнародну правові системи.

7. Своєчасно вжиті юридичною науковою спільнотою зусилля можуть дозволити отримати попереджувальні наукові результати і практичні рекомендації щодо правового регулювання суспільних відносин, що сприятиме широкому визнанню, швидкому впровадженню і поширенню прогресивних досягнень чергової технологічної революції, в тому числі, технологій Інтернету речей і технологій блокчейн.

Розділ ІІ

ПРАВОВІ ПРОБЛЕМИ ЗАСТОСУВАННЯ РОЗУМНИХ КОНТРАКТІВ

Історичні передумови застосування розумних контрактів
Становлення поняття “розумний контракт” (smart contract)
Особливості визначення smart contract для юридичних досліджень
Класифікація smart contract у правовому контексті
Проблеми визначення юридичної сили smart contract
Спільні та відмінні риси традиційного та
розумного контракту
Виконання, внесення змін та розгляд
спорів у smart contract
Проблеми формування правового забезпечення
smart contract

Історичні передумови застосування розумних контрактів

Світ знаходиться на порозі початку тотального використання технологій Інтернету речей, орієнтованих на дистанційне надання послуг і проведення робіт в найрізноманітніших сферах людської діяльності за участю або без участі людей, але в інтересах фізичних і юридичних осіб. У цих умовах особливого значення набуває можливість за участю або без участі людини дистанційно укладати і виконувати договори на основі використання інформаційно-комунікаційних технологій, які отримали назву розумні контракти. Тому останнім часом увагу багатьох вчених і практиків привертає проблематика розумних контрактів.

Ще в 1997 році М. Сабо констатував, що наслідки розробки розумних контрактів відповідно до договірного права, а також розробки стратегічних контрактів на середину 1990-х років мало вивчені, незважаючи на величезні перспективи, особливо у разі використання елементів штучного інтелекту, які також мало вивчені [24].

В даний час розумні контракти досить широко, як для нового явища, увійшли в практику договірних відносин. Найбільш яскравим прикладом може служити біткойн, як всесвітня пірінгова криптовалютна цифрова платіжна система, яка використовує однойменну розрахункову одиницю і однойменний протокол передачі даних. Але, тим не менш, не уявляється можливим констатувати якісь значні успіхи юридичної науки в дослідженні проблематики розумних контрактів за минулі 20 років.

У дискусії про розумні контракти можна умовно виокремити два основних підходи: розумні контракти – це коли суспільні відносини регулюються програмним забезпеченням (комп'ютерним кодом) [25];

розумні контракти – це коли при реалізації суспільних відносин використовується програмне забезпечення, що відповідає певним домовленостям або положенням закону.

Відносно першого підходу викладемо такі міркування. Відомо, що люди (програмісти) створюючи програмне забезпечення, керуються певними алгоритмами реалізації якихось дій (обчислень, обробки даних, функціонування технічних виробів, поведінки людей тощо). Ці алгоритми створюються людьми, які відображають в них своє розуміння порядку або правил реалізації певних дій, але розуміння, яке детермінується відомими закономірностями математики, фізики, механіки, металообробки, електроніки, робототехніки тощо, а в разі людей – соціальними регуляторами, в тому числі – правовими нормами.

Таким чином, поки програмні засоби для розумних контрактів створюються людьми або під керівництвом людей можна сміливо стверджувати, що перший підхід, який базується на твердженні – "суспільні відносини регулюються програмним забезпеченням", принципово спотворює сприйняття ролі та місця комп'ютерних кодів в суспільних відносинах.

Однак слід зауважити, що незважаючи на таку фундаментальну методологічну помилку деяких авторів – прихильників цього метафізичного підходу, не можна безапеляційно повністю відкидати отримані ними наукові результати, частина з яких може бути досить продуктивною для розвитку юридичної теорії та практики розумних контрактів.

Виходячи з вище викладеного, в цій роботі буде приділено увагу розвитку другого підходу. На наш погляд, дослідження теоретико-методологічних і законодавчих проблем правового регулювання застосування інноваційних розумних контрактів, особливо в умовах широкого використання технологій Інтернету речей з метою створення сприятливих умов для їх широкого застосування в людській і юридичній практиці, є актуальним завданням.

Становлення поняття "розумний контракт" (smart contract)

Історично першим було визначення сформульоване Н. Сабо: "розумний контракт – це набір обіцянок, зазначених в цифровій формі, включаючи протоколи, в якій сторони виконують ці обіцянки" [24].

Але в сучасній юридичній літературі як немає досі єдиного визначення Інтернету речей, так немає і єдиного визначення терміну "розумний контракт". Наприклад дають таке визначення: розумний контракт – це договір, який існує в формі програмного коду, що імплементовано на платформі Blockchain, який забезпечує автономність і самовиконання умов такого договору у разі настання заздалегідь визначених в ньому обставин [26].

Головна мета створення розумного контракту – автоматизація взаємовідносин різних сторін, побудована на основі алгоритму, якому кожна зі сторін надала право від свого імені здійснювати певні дії відповідно до низки вимогливо заданих умов. Іншими словами, розумний контракт – це одночасно і набір правил, і робот, який від імені свого "господаря" вчиняє дії за заданими правилами, в тому числі такі, що впливають на правовідносини [27].

Старк Д. вважає, що термін "розумний контракт" відноситься до випадку використання комп'ютерного коду у вигляді мови програмування, наприклад javascript або HTML, для формулювання, перевірки і виконання угоди між сторонами, що фактично стає еквівалентною заміною контракту, написаного природною людською мовою [28]. При цьому розумний контракт "виконується" комп'ютером з урахуванням умов угоди.

В роботі, присвяченій транскордонним аспектам, вважається, що розумні контракти – це програмні коди, в які вбудовуються умови контракту і які працюють в мережі, що призводить до

часткового або повного автоматизованого самовиконання контракту [29].

Смарт-контракти – це угоди, що виконуються автоматизовано за допомогою комп'ютерних програм, що мають контроль над фізичними або цифровими об'єктами, реалізація яких відбувається без людського впливу і звернення до суду [30].

Отже, аналізуючи наведені та багато інших дефініції визначення "розумний контракт", можемо виділити те спільне, що їх об'єднує: це набір обіцянок, зазначених в цифровій формі; це набір правил; це договір, який існує в формі програмного коду, що імплементовано на платформі блокчейн (; це договір, який самостійно виконується у разі настання заздалегідь визначених в ньому обставин; це набір комп'ютерного коду, який використовується для формулювання, перевірки і виконання договору; це програмні коди, в які вбудовуються умови контракту і які працюють в мережі і є еквівалентною заміною контракту, що "виконується" комп'ютером; це угоди, що виконуються автоматизовано за допомогою комп'ютерних програм, реалізація яких відбувається без людського впливу.

Слід зауважити, що всі дефініції визначення "розумний контракт" безпосередньо або опосередковано в наступних поясненнях містять посилання на використання технології або платформи блокчейн. Це можна пояснити тим, що саме з розробкою технології блокчейн-ланцюжків створилася можливість більш-менш ефективно втілити в життя ідею розумних контрактів, завдяки особливим властивостям цієї технології.

Особливості визначення smart contract для юридичних досліджень

З метою формулювання дефініції терміну "розумний контракт" в юридичній конотації вважаємо недоцільним згадку в цій

назви конкретної технології виходячи з принципу технологічної нейтральності правового регулювання. Технології можуть детермінувати особливості правового регулювання, але не визначати його сутність. Інакше з появою кожної нової технології довелося б переписувати закони. А як бути, коли в соціальних відносинах буде одночасно використовуватися набір різних технологій? Тому в подальших дослідженнях будемо розглядати приклади з використанням блокчейн-ланцюжків тільки з метою визначення особливостей правового регулювання при їх використанні в договірних відносинах.

Сформулюємо в інтересах юридичних досліджень таку дефініцію: розумні контракти – інноваційна форма контрактів, укладення, виконання та припинення яких відбувається за участю або без участі людини, але з використанням мережевих комп'ютерних програмних та/або програмно-апаратних засобів, що мають взаємозв'язок з фізичними або цифровими об'єктами.

Відмінною рисою цього визначення є те, що розумний контракт визнається еквівалентом традиційного контракту, який за допомогою ІКТ може укладатися, виконуватися і припинятися за участю або без участі людини. Участь людини може проявлятися навіть в простому ініціюванні виконання розумного контракту. Крім того, це визначення інваріантне до типу використовуваних технологій і до типу використовуваних мов програмування.

Зазвичай, в літературі вказують на такі переваги застосування розумних контрактів, заснованих на використанні блокчейнів [31]:

Ц висока швидкість – використання смарт-контрактів, дозволяє значно прискорити бізнес-процеси.

Ц ефективність – для повторюваних, однотипних контрактів.

Ц достовірність – принцип побудови блокчейн-ланцюжків виключає внесення змін до його тексту змін, не санкціонованих усіма сторонами контракту.

Ц спостережність – прозорість і простота звітності про вчинені транзакції.

Ц економічність – зменшення транзакційних витрат завдяки виключенню посередників, зменшення витрат людської праці.

Ц надійність – мінімізація ризику виникнення механічної помилки в процесі виконання контракту, можливість відновлення даних у разі їх втрати, висока стійкість проти кіберзагроз.

Ц універсальність – можливість застосування в найрізноманітніших сегментах людської діяльності.

Справедливості заради, слід зазначити, що не всі поділяють ентузіазм з приводу розумних контрактів.

Деякі дослідники вважають, що на даному етапі "розумний" контракт здебільшого являє собою кращий спосіб автоматизованого виконання досягнутих домовленостей, такий своєрідний спосіб їх виконання, ніж традиційний контракт (договір), що представляє собою сформульований набір домовленостей сторін, які досягнуті за допомогою переговорного процесу. Таким чином, вони припускають, що можливий сценарій, відповідно до якого сторони укладають звичайний договір та передбачають в ньому механізми виконання із застосуванням автоматизованих алгоритмів ("розумних" контрактів). Разом з тим, вони стверджують, що звичайний "паперовий" договір повинен в будь-якому випадку мати пріоритет над "розумним" контрактом [32].

Смарт-контракти можуть також спричинити нові проблеми, вважають в юридичній фірмі Strafford Kent Law (Nottingham, England), а деякі варіанти їх використання просто неможливі. В результаті юридичного аналізу вони доходять такого висновку: в реальному житті складно розглядати інтелектуальний контракт як розумний, так і як контракт тому, що в даний час це просто автоматизований комп'ютерний код. Отже, застосування терміну "розумний контракт" певним чином вводить в оману, тому, можливо, краще відмовитися від нього. Більш відповідною назвою, ймовірно, буде інтелектуальний агент або інтелектуальна програма.

Напевно, важко повною мірою опротестувати такі висновки, оскільки ряд практичних кейсів, які сьогодні називають розумними

контрактами, такими дійсно не є, але, в той же час, з'являється дедалі більше прикладів дійсно розумних контрактів, які повністю виконуються за допомогою мережевих комп'ютерних програмних та/або програмно-апаратних засобів. Тому реальні чи уявні перспективи застосування стимулюють проведення правових наукових досліджень в сфері застосування розумних контрактів.

Класифікація smart contract у правовому контексті

Зазвичай наукові дослідження починаються з вивчення питань класифікації, що дозволяє згодом провести певну декомпозицію об'єкта дослідження і спростити його вивчення. У проблематиці розумних контрактів було запропоновано класифікувати їх на сильні і слабкі [30]. На думку М. Раскіна під сильними розумними контрактами слід розуміти ті, для яких їх анулювання та модифікація призводять до надмірно високих витрат, а слабкі розумні контракти – це ті, які таких витрат не мають. Далі несподівано з'являється парадоксальний висновок про те, що суду не має сенсу своїм рішенням змінювати сильний контракт після його виконання, оскільки це призведе до непомірно високих витрат.

У багатьох юрисдикціях сторонам договору надається конституційне право на звернення до суду для захисту своїх інтересів або порушених прав. Тому запропонований підхід призводить до ситуації оцінки розумних контрактів тільки як слабких, тобто таких, в яких всі дії сторін строго детерміновані та не допускають неоднозначного розвитку подій, що вимагає певного вибору для кожної зі сторін, а це, на нашу думку, різко звужує можливі сфери застосування розумних контрактів.

Тому запропонуємо класифікувати розумні контракти на саморегульовані і на регульовані відповідно до загального договірного права.

З огляду на поширений в національних юрисдикціях принцип свободи договору є цілком логічним припущення, що певна спільнота суб'єктів може встановити всередині себе деяку сукупність правил здійснення розумних контрактів, що прямо не передбачені законодавством, але і не суперечать договірному праву, які дозволяють мінімізувати контрактні помилки, що призводять до виникнення спірних ситуацій.

Спільноту, в якій регулювання всіх суспільних відносин здійснюється на основі нею створених правил, будемо називати саморегульованою, а розумні контракти, які будуть використовуватися для формалізації взаємовідносин між членами цієї спільноти, будемо називати саморегульованими розумними контрактами.

Крім того, співтовариство в рамках своїх правил також може встановити порядок розгляду можливих спорів без звернення до суду. Такий підхід дозволяє істотно скоротити витрати, пов'язані з судовим розглядом суперечок, в будь-якій предметній сфері застосування розумних контрактів.

Таким чином, м'яке право, виражене в правилах саморегульованої спільноти матиме високу ефективність, якщо оголошені правила в частині укладення, виконання та припинення розумних контрактів не містять внутрішніх протиріч, які можуть стати причиною виникнення суперечок, і приймаються беззастережно всіма членами спільноти. Як показує практика, такий підхід досить успішно реалізується в закритих пірінгових платіжних системах.

У той же час, правила саморегульованої спільноти повинні бути такими, щоб забезпечувати юридично дозволену поведінку її членів з метою мінімізації втручання державних інституцій, наприклад, в разі правопорушень. З юридичної точки зору система правового регулювання взаємовідносин саморегульованої спільноти з кандидатами в її члени може мати в якості аналогії публічний договір.

Однак при цьому доцільно розробити вичерпні, прозорі і не надмірні правові механізми для проведення, в разі необхідності, інспектування правоохоронними органами на відповідність закону предметів розумних контрактів, які виконуються в межах саморегульованих спільнот, з мінімізацією або виключенням порушення виконання цих контрактів та з встановленням юридичної відповідальності для посадових осіб за зловживання владою.

Проблеми визначення юридичної сили smart contract

Цілком очевидно, що необхідно провести дослідження для виявлення особливостей системи правового регулювання в різних галузях застосування розумних контрактів за умови використання мережевих комп'ютерних технологій з метою максимального зменшення транзакційних витрат і зниження бар'єрів при розгляді спорів в суді. Перш за все, звичайно, необхідно визначитися з юридичним статусом розумного контракту як контракту, який укладається, виконується і припиняється з використанням мережевих комп'ютерних програмних та/або програмно-апаратних засобів.

У деяких роботах пропонується визнавати юридичний статус розумних контрактів відповідно до положень Конвенції ООН про використання електронних повідомлень у міжнародних договорах на підставі наступного [33]:

Ц розумний контракт формується в електронному вигляді за допомогою комп'ютерного коду (стаття 1);

Ц розумні контракти, сформовані в результаті автоматичних повідомлень, є юридично дійсними та підлягають виконанню відповідно до Конвенції (стаття 12).

В результаті критичного аналізу можна констатувати, що: положення Конвенції поширюються на використання автоматизованих

систем повідомлень, але повідомлень, які викладені природньою мовою, оскільки в Конвенції згадується “про взаємодію автоматизованої системи повідомлень і будь-якої фізичної особи...”. Тому положення Конвенції не можуть застосовуватися до випадків з повідомленнями, представленими виключно у вигляді програмного коду.

Таким чином, уявляється помилковою пропозиція щодо визнання юридичної сили розумного контракту на підставі положень Конвенції ООН про використання електронних повідомлень в міжнародних договорах.

Цивільний кодекс України встановлює, що в письмовій формі повинні укладатися всі контракти між юридичними особами, юридичними і фізичними особами (за винятком усних), між фізичними особами, якщо сума договору двадцятикратно перевищує розмір неоподатковуваного мінімуму.

У статті 207 ЦКУ законодавець встановив умови того, коли контракти, вчинені з використанням електронних документів, можуть вважатися укладеними в письмовій формі. Ці вимоги, звичайно, відносяться до документів (інформаційних повідомлень) викладених природньою мовою. При цьому допускається використання спеціального електронно-цифрового підпису, який відповідно до закону є еквівалентом власноручного підпису.

Виходячи з цього, виникає проблема необхідності розробки правових механізмів для розумних контрактів в частині:

- визнання “тексту” договору, викладеного в комп’ютерному коді, еквівалентним письмовій формі;
- визнання систем верифікації сторони контракту, які використовуються в мережевих комп’ютерних програмних та/або програмно-апаратних засобах, еквівалентними законодавчо схваленим системам ідентифікації суб’єктів за допомогою електронного або електронно-цифрового підпису;

- визначення місця укладення контракту з урахуванням можливої різної національної юрисдикції і мобільності сторін договору, наприклад, якщо сторона договору перебуває на борту літака, що летить;
- нотаріального посвідчення та державної реєстрації розумних контрактів.

Таким чином, для розумних контрактів, які повністю ускладаються та/або виконуються за допомогою мережевих комп'ютерних програмних та/або програмно- апаратних засобів, реалізованих з використанням певної мови програмування, необхідно провести ретельний аналіз системи правового регулювання в частині забезпечення формальних вимог до укладання контрактів. Це стосується, перш за все, вимоги щодо письмової форми укладання контракту, нотаріального засвідчення та державної реєстрації контракту, визначення місця укладення контракту тощо.

Різні етапи договірних відносин (укладення, виконання та припинення) мають різний ступінь ризику виникнення суперечок.

На першому етапі договірних відносин в переважнійбільшості випадків ймовірність виникнення спору дуже низька, оскільки сторонидобровільно погоджуються на виконання умов, обговорених в контракті, в тому числі й в розумному.

У національних юрисдикціях, як правило, закріплено принцип презумпції правомірності укладених контрактів, як, наприклад, в статті 204 Цивільного кодексу України. Винятки становлять лише пряма вказівка в законі на недійсність договору або якщо недійсним його визнає суд. Крім того, в законодавстві формулюють загальні вимоги, виконання яких є обов'язковим для того, щоб контракт вважався дійсним, наприклад, відсутність суперечності законодавству, наявність цивільної дієздатності, вільне волевиявлення, дотримання встановленої форми укладення, націленість на досягнення реальних правових наслідків тощо.

Однак найбільша кількість суперечок може виникати на етапі виконання. Це пов'язано, як це часто буває в реальній практиці виконання контрактів, з необхідністю узгодженої зміни певних умов його виконання або зміни загальних умов його виконання, що потребує створення юридичних і технологічних можливостей для внесення змін в розумні контракти шляхом зміни програмного забезпечення. Оскільки доктрина загального права щодо реального виконання дозволяє визнати контракт навіть в тому випадку, якщо його виконання не в повному обсязі відповідає викладеним в ньому певним умовам [30], то внесення таких змін може бути не обов'язковим, що надає можливість сторонам провести дослідження в кожному конкретному випадку для відносної оцінки необхідних витрат на модернізацію розумного контракту й шкоди для сторін в разі відсутності зміни програмного забезпечення.

Як вже раніше зазначалося, у всіх відомих на сьогодні прикладах застосування розумних контрактів укладення, виконання та припинення відбувається з використанням мережевих комп'ютерних програмних та/або програмно-апаратних засобів, які реалізовані на технології (платформі) блокчейн-ланцюжків. Застосування блокчейн-платформ для реалізації розумних контрактів призводить до необхідності дослідження особливостей правового регулювання використання розумних контрактів.

Одним з ключових питань для урядів є питання про те, чи повинні законодавчі положення регулювати всі потенційні застосування технології блокчейн або повинні обмежуватися лише певними галузями і випадками їх застосування. Банківська і фінансова індустрія є наочним прикладом галузі, яка, ймовірно, вдасться до жорстких заходів контролю щодо технологій, заснованих на технології "блокчейн" [8].

Серед експертів існують різні точки зору на оцінку можливого використання розумних контрактів.

Деякі з них вважають, що найбільші перспективи має модель, коли розумні контракти реалізуються в рамках традиційної правової системи, визнаючи при цьому, що розумні контракти не повинні замінювати ні традиційне договірне право, ні традиційних юристів за контрактом [33]. Крім того, вони вважають, що традиційне договірне право, зокрема вимоги до правил доведення, можливо, необхідно буде змінити, з урахуванням автоматизованого і детермінованого характеру розумних контрактів, а також питань, пов'язаних з можливістю їх реалізації.

Спільні та відмінні риси традиційного та розумного контракту

Поява розумних контрактів, швидше за все, може призвести до переоцінки загальноприйнятої практики договірного права в міру того, як юристи будуть визначати, які типи угод і термінів найкраще підходять для програмування та автоматичного виконання, а які слід залишити для складання природною мовою [28].

Проаналізуємо можливі відмінності або схожість в процесі складання розумного контракту і традиційного контракту як угод про реалізацію суспільних відносин в якійсь предметній сфері.

При укладанні, виконанні та припиненні будь-якого контракту, який визнається національною або міжнародною правовою системою, сторони мають на меті зробити і роблять певні дії, детерміновані правовими нормами контракту або законодавства, відповідно до певного алгоритму, зміст якого великою мірою визначається власне конкретним типом контракту. Або, іншими словами, будь-який контракт є описом алгоритму дій його сторін при взаємодії одна з одною для досягнення мети контракту. В даному випадку алгоритм означає певну послідовність дій сторін контракту, що здійснюються в рамках традиційної системи права відповідно до класичної структури правової норми: гіпотеза,

диспозиція і санкція. У класичній лексиці алгоритмів структура правової норми виглядає так:

- ***якщо*** – опис гіпотези як опису деякої сукупності зовнішніх і внутрішніх умов або опису стану сторін, які є виключною підставою для початку виконання окремих елементів контракту;
- ***то*** – опис диспозиції як опису сукупності певного набору дій сторонами контракту, які обов'язково виконуються при настанні умов, описаних гіпотезою;
- ***інакше*** – опис санкцій як опису деякої сукупності дій по відношенню до сторони контракту, що не виконала вимог диспозиції, які дозволяють компенсувати збитки, завдані іншій стороні невиконанням положень контракту.

Ухвалення формального алгоритмічного підходу, обґрунтованого самою структурою правових норм, при складанні комп'ютерної програми, що реалізує укладання, виконання і припинення розумного контракту відкриває шляхи до найрізноманітніших способів перетворення природної юридичної мови (мови складання традиційного контракту) в мову (лексику) програм, "зрозумілих" обчислювальним машинам. Оскільки розумні контракти передбачають використання ІКТ, то ця обставина уявляється досить важливою.

Таким чином, можемо висунути гіпотезу про те, що існує принципова можливість еквівалентного перетворення алгоритму дій, який закладається в традиційний контракт за допомогою викладання правових норм природньою юридичною мовою, у відповідний комп'ютерний алгоритм, що створює сприятливі умови для подальшого створення контрактів у вигляді комп'ютерних програм (комп'ютерних кодів).

Для визначення вимог до апаратно-програмного забезпечення розумних контрактів Н. Сабо виділяє чотири необхідних функціональних властивості звичайних контрактів [24]:

1. Спостережність – здатність сторін спостерігати за виконанням контракту іншою стороною або доводити свою ефективність третім особам.

2. Верифікованість – здатність сторін контракту довести арбітру, що контракт був виконаний або порушений, або здатність арбітра визначити це іншими способами.

3. Спостережність та верифікованість створюють умови для своєчасної індикації навмисних порушень контракту або помилки сумлінності.

4. Секретність (privity) – принцип, згідно з яким знання та контроль за змістом і виконанням контракту повинні розподілятися між сторонами лише в тому обсязі, наскільки це необхідно для виконання цього контракту.

5. Здатність до виконання – реалістичність виконання контракту, що мінімізує необхідність в забезпеченні дотримання виконання контракту.

Деякі дослідники вважають, що оскільки транзакції розумного контракту запрограмовані в блокчейне, то закодований характер дозволяє сторонам висловлювати умови контракту менш складними способами, ніж якби умови були написані простою мовою на папері.

Інші ж автори вважають, що сфера застосування розумних контрактів обмежена, оскільки контракти природньою мовою завдяки багатій семантиці дозволяють моделювати життєві ситуації з досить великим ступенем абстракції [27, 32].

Але велика ступінь абстракції – це скоріше недолік, а не перевага контрактів укладених природньою мовою, оскільки вона обумовлює великий ступінь невизначеності при виконанні контрактів, що неминуче може призводити і призводить до виникнення суперечок. На проблему наявності розриву між семантикою юриста і оперативною семантикою програміста, яка може призвести до неприйнятних операційних і нормативних ризиків, звертає увагу ряд авторів [34], що також може бути

причиною суперечок при реалізації розумного контракту у вигляді програмного забезпечення. Необхідність вирішення спорів збільшує для всіх сторін як вартість окремих контрактних транзакцій, так і вартість контракту в цілому.

Слід зауважити, що причини для деяких суперечок від самого початку закладаються в традиційні контракти завдяки застосуванню категорій, які неоднозначно визначаються і сприймаються, таких як: "відповідають прийнятим стандартам", "відповідно до прийнятих правил", "сумлінна практика", "розумний строк" тощо. Це відбувається, як правило, внаслідок того, що юристи недостатньо ретельно підходять до написання текстів контрактів або недостатньо ретельно опрацьовують його положення. Переклад контрактів (алгоритму контракту) з природної мови в машинну (комп'ютерну програму) закономірно призводить до необхідності або точного опису таких категорій чи інших термінів, або їх заміни іншими категоріями чи термінами, які точно і однозначно сприймаються, або виключення таких категорій з тексту контракту. А це, в цілому, тільки покращує правові умови виконання контрактів роблячи їх більш прозорими і логічними, що призводить до зменшення ризиків збільшення вартості контрактних транзакцій за рахунок виникнення суперечок.

Ідентифікація та аналіз джерел і причин збільшення вартості контрактних транзакцій повинні скласти окремий предмет правових досліджень, результати якого можуть позитивно вплинути на широту застосування розумних контрактів.

Залежно від складності конкретної контрактної діяльності комп'ютерні програмні та/або програмно-апаратні засоби, за допомогою яких реалізуються розумні контракти, можуть набувати складної структури і мати багато тисяч рядків виконуваних машинних кодів. В цьому випадку готова програмна реалізація, можливо, буде працювати не так як це проектувалося її розробниками, тобто результати її роботи не відповідатимуть алгоритму контракту. Крім того, у величезному масиві програмних

кодів вірогідна поява механічних помилок, які не завжди можуть проявлятися в процесі налагодження програми. Один з яскравих прикладів – це операційна система Windows, поновлення до якої, викликані необхідністю усунення помилок, виходять практично щотижня.

Вважають, що будь-який розумний контракт з тисячами умов і вкладених операторів перемикання типу “якщо..., то..., інакше...” може бути протестований для кожної умови або кожного оператора перемикання, наявного в комп’ютерній програмі, що виконує контракт, тобто аналогічно тому, як розробники програмного забезпечення “налагоджують” свій власний код, перевіряючи його у всіх можливих обставинах, юристи зможуть перевіряти контракти, даючи кожній стороні угоди більш чітке розуміння свого ризику [28].

Тому існує необхідність створення правових механізмів реагування на випадки неправильного виконання контракту внаслідок наявності помилок в програмному забезпеченні, які можуть бути виявлені на будь-якому етапі життєвого циклу розумного контракту.

В цілому, можна визнати, що перетворення алгоритму дій, який відображається в традиційному контракті, у відповідну комп’ютерну програму представлятиме один з основних бар’єрів на шляху широкого поширення розумних контрактів в різних сегментах соціуму.

Отже, вважаємо за доцільне створення в майбутньому систем автоматизації програмування розумних контрактів, зрозумілих для використання юристами без наявності спеціальної освіти в програмуванні. Для цього необхідно провести дослідження з розробки предметно-орієнтованих на юридичну сферу надвисокорівневих мов програмування з високим рівнем абстракції або програмування природньою мовою з використанням штучного інтелекту, в тому числі, можливо, і з використанням рекурентної нейронної мережі [35].

Виконання, внесення змін та розгляд спорів у smart contract.

При виконанні розумного контракту можуть мати місце випадки необхідності скасування контракту, наприклад, тому, що його було укладено під примусом або за інших обставин, які традиційне договірне право визнає підставою для невизнання контракту. Деякі автори вважають, що, імовірно, незворотні транзакції можуть бути просто компенсовані подальшою транзакцією, що приводить все до початкового стану.

Очевидно, таке припущення викликано розумінням того, що ретельно складений і алгоритмізований контракт після переведення його на одну з мов програмування зажадає значних зусиль для його оперативної зміни. Однак, цілком можлива розробка алгоритмів, досить гнучких до зміни умов, але це вимагатиме реалізації інноваційних підходів.

Інший приклад, який ілюструє необхідність забезпечення можливості внесення змін до розумного контракту, пов'язаний з використанням технології блокчейна в управлінні ланцюгами поставок, що тягне за собою серйозні проблеми для правового регулювання. Такі правила, як європейська директива про нефінансову звітність, можуть вплинути на використання ланцюжків блокчейна в процесі поставок, оскільки при цьому від компаній вимагається розкриття достовірної інформації з екологічних питань, соціальних аспектів та аспектів роботи співробітників, дотримання прав людини та вимог щодо боротьби з корупцією з метою підвищення прозорості їх діяльності. Однак відсутність посередника на більшості або всіх етапах ланцюжка поставок в майбутньому може створити невизначеність для залучених сторін, особливо коли мова йде про автоматизовані форми виконання та нагляду за транзакціями. У більшості випадків

необхідно враховувати поняття та механізми юридичної відповідальності або юридичної відповідальності при виникненні непередбачених проблем тому, що якщо вони не враховані, то контракт повинен бути допрацьований [31].

Створення юридичних і технологічних можливостей для внесення змін в розумні контракти шляхом зміни програмного забезпечення може бути також обумовлено тим, що в процесі розгляду спорів або оцінки відповідності змісту контракту вимогам законодавства суди можуть виносити рішення про зміну умов виконання розумного контракту або навіть про визнання недійсним договору (стаття 215 ЦКУ).

Однією з важливих проблем застосування розумних контрактів є правозастосовність та можливість розгляду спорів в суді. Це обґрунтовується тим, що багато галузей, де можливе використання розумних контрактів, наприклад, галузь фінансових послуг, мають досить детальне правове регулювання, в тому числі, яке передбачає наявність для учасників угод спеціальних ліцензій та дозволів.

Крім того, на наш погляд, потрібно приділити серйозну увагу питанням, пов'язаним з розглядом суперечок в суді, наприклад, питанням юридичної фіксації та протоколювання всіх зовнішніх чинників, що впливають на виконання контракту в автоматичному режимі, можливості проведення експертизи на відповідність комп'ютерної програми алгоритму виконання контракту, який вона реалізує тощо.

Для розгляду спору в суді, як і для багатьох інших випадків, які сьогодні передбачаються традиційною системою права, необхідна наявність тексту розумного контракту, викладеного природньою юридичною мовою. Таким чином, необхідна правова регламентація трансляції (перекладу) комп'ютерної програми, що містить опис розумного контракту, природньою юридичною мовою. Правові механізми регулювання такої трансляції можуть бути

аналогічні існуючим правовим механізмам здійснення перекладу з іноземних мов.

Розгляд в суді суперечок, пов'язаних з розумними контрактами, завжди буде знаходитися на стику проблем, пов'язаних з правовим регулюванням, і проблем їх інтерпретації в лексиці програм, "зрозумілих" обчислювальним машинам, а також проблем відповідності алгоритмів програмного забезпечення алгоритмам правового регулювання.

Тому закономірно виникає питання про необхідність формування корпусу суддів, що повинні володіти відповідними компетенціями для розгляду спорів, обтяжених застосуванням комп'ютерних технологій, і наявності інституту кваліфікованих експертів.

Особливу увагу для випадку застосування розумних контрактів в технологіях Інтернету речей слід приділити питанням взаємодії мережевих комп'ютерних програмних та/або програмно-апаратних засобів, за допомогою яких реалізуються розумні контракти, з фізичними або цифровими об'єктами, зміна стану яких буде виступати своєрідним тригером (спусковим механізмом) для вступу в дію тих чи інших положень контракту. В цьому випадку будуть мати місце проблеми правового регулювання верифікації фізичних або цифрових об'єктів, забезпечення кібербезпеки технологічних систем взаємозв'язку зовнішніх об'єктів з розумними контрактами, підтвердження достовірності та цілісності, а також протоколювання переданих повідомлень. Крім того, виникають проблеми правового визначення юридичних механізмів анонімізації фізичних об'єктів з метою забезпечення захисту персональних даних.

Ще один ймовірний суттєвий бар'єр у взаємодії розумних контрактів з фізичними або цифровими об'єктами було визначено в одній з робіт, в якій зазначається, що кожен вузол в ланцюжку блокчейнів виконує розумні контракти незалежно (вірніше, дублюючи їх), але не синхронно, тому, коли виникає необхідність

використання інформації від зовнішнього джерела, то кожен вузол робить це повторно і окремо [15]. Автори роботи стверджують, що оскільки це джерело знаходиться поза блокчейн- ланцюгом, то немає гарантії, що кожен вузол отримає одну і ту саму інформацію, оскільки фізичні або цифрові об'єкти можуть в різний час генерувати різну інформацію про свій стан або стати тимчасово недоступними. Наявність відмінностей в інформації, яка записується в вузли блокчейн-ланцюжка, призводить до відмови в транзакції, тобто у відмові виконання якихось положень розумного контракту. Ця проблема вимагає вирішення як на технологічному, так і на правовому рівні.

При використанні розумних контрактів питання забезпечення кібербезпеки стають пріоритетними, як і для всіх технологій, заснованих на використанні ІКТ та мережі Інтернет. У 2016 році Децентралізована автономна організація (Decentralized Autonomous Organization, DAO) оголосила, що хакер використав уразливість в Ethereum-платформі, що використовує блокчейн, завдавши загальний збиток близько 150 мільйонів доларів. Але недолік був не в самій платформі блокчейна, а в наявності лазівки в коді розумного контракту, тому хакеру вдалося створити рекурсивну відправку грошей в контракті, тобто команда відправки коштів викликала інший запит "відправити гроші" [36].

Незважаючи на те, що в даному конкретному випадку платформа, яка використовує блокчейн, виявилася поза підозрою, питання забезпечення надійності її функціонування залишається відкритим. Як інфраструктурна основа для багатьох додатків розумного контракту, вона повинна відповідати підвищеним вимогам до надійності, безперервності і стійкості роботи, а також до стійкості в умовах реалізації кіберзагроз.

Відомо, що кожен вузол в блокчейн-мережі зберігає величезні обсяги одних і тих самих даних і, в залежності від застосування блок-ланцюга, деякі з цих даних можуть бути класифіковані як персональні дані, що створює певні труднощі із застосуванням

законодавства в частині недопущення несанкціонованої та незаконної обробки персональних даних і недопущення їх випадкової втрати або знищення, а також в частині задоволення законної вимоги про їх видалення.

З урахуванням того, що в цілому технології Інтернету речей при наданні послуг і проведенні робіт будуть характеризуватися превалюванням горизонтальних зв'язків між суб'єктами, особливої актуальності набуває вивчення проблеми можливості використання розумних контрактів в транскордонному режимі. Розумні контракти, що базуються на використанні блокчейн-платформ, максимально підходять для підтримки горизонтальних взаємозв'язків між суб'єктами договірних відносин і дозволяють здійснювати транзакції в транскордонному режимі, що призводить до необхідності вирішення проблеми визначення юрисдикції цих контрактів.

З входженням в життя соціуму нових технологій, в тому числі і інформаційних, практично завжди виникає питання про реакцію системи права на використання цих технологій в суспільних відносинах. Традиційно ця реакція зводиться до чотирьох варіантів: нічого не треба змінювати; потрібні лише деякі косметичні зміни в праві і законодавстві; необхідні, іноді суттєві, зміни положень традиційної системи права і законодавства; створення нових галузей права і законодавства.

Вельми спокусливим виглядає четвертий варіант, який, здавалося б, створює умови для реалізації можливості креативно та інноваційно підійти до вирішення проблем правового регулювання суспільних відносин, які виникають у зв'язку з використанням нових технологій. В останні роки такий підхід набув поширення у вигляді пропозицій про створення нових галузей права, наприклад таких як: право електронних магістралей, телекомунікаційне право, право IT, комп'ютерне право тощо. Звичайно, подібні ідеї мають право на життя, але за умови: по-перше, серйозного теоретичного

обґрунтування можливості виділення окремої нової галузі права, по-друге, обґрунтування практичної та економічної доцільності.

Нові технології широко входять в практику суспільних відносин – це, як правило, проривні технології, що ведуть до прогресу в розвитку соціуму. З урахуванням сучасної динамічності розвитку суспільних та економічних процесів, часу на створення систем правового регулювання з урахуванням використання цих нових технологій відводиться не дуже багато. З іншого боку, відсутність ефективної системи правового регулювання є одним з основних бар'єрів на шляху широкого використання нових технологій в суспільних відносинах, що може бути причиною зниження темпів економічного розвитку. Тому для багатьох сучасних стратегій розвитку системи права в зв'язку з появою нових технологій, наприклад, технологій Інтернету речей або розумного контракту, та їх використання для реалізації суспільних відносин найбільш ефективним є третій варіант:
внесення необхідних змін в традиційну систему права і систему законодавства.

У частині розумних контрактів слід підтримати позицію Сабо Н., яка кореспондується з нашим попереднім висновком: "успіх загального права контрактів в поєднанні з високою вартістю його заміни робить доцільним як збереження, так і використання принципів цього права там, де це необхідно" [24].

Проблеми формування правового забезпечення smart contract

Таким чином, в частині вирішення проблеми формування правового забезпечення широкого застосування розумних контрактів з урахуванням викладеного раніше і результатів деяких досліджень [24, 31] можна сформувати наступні завдання, що стоять перед правою наукою:

1. Інтеграція системи правового регулювання застосування розумних контрактів, що буде розроблятись, в традиційну національну правову систему.

2. Визначення юридичного статусу розумного контракту, формування правових вимог до його форми і змісту.

3. Визначення юрисдикції розумних контрактів, в тому числі, за наявності транскордонних транзакцій.

4. Дослідження особливостей правовідносин, пов'язаних з розумними контрактами, юридичних прав, обов'язків і відповідальності його сторін.

5. Дослідження проблеми визначення юридичних ризиків та обмежень використання розумних контрактів в різних сферах застосування.

6. Формування правових механізмів нагляду, встановлення відповідальності за порушення умов розумного контракту і відшкодування завданих збитків або за наявності помилок в комп'ютерній програмі.

7. Формування правових вимог щодо забезпечення достовірності індикації та фіксації подій або явищ в реальному світі, факт наявності яких є причиною для здійснення певних дій сторін при виконанні розумного контракту.

8. Розв'язання правовими засобами проблеми наявності неповної можливості для учасників договору спостерігати за всіма прихованими діями програмного забезпечення розумного контракту, що може призвести до небажаного збитку.

9. Розробка правових механізмів верифікації сторін контракту, що здійснюють транзакцію, на момент її здійснення.

10. Розв'язання протиріччя між законодавчими вимогами обмеження доступу до персональних даних та іншої чутливої інформації сторін контракту, яка в ньому може міститися, і відкритістю інформації за всіма транзакціями для всіх учасників публічної децентралізованої мережі блокчейнів і її зберіганням в кожному вузлі блокчейн- ланцюжка.

11. Правова регламентація забезпечення кібербезпеки як програмного забезпечення, що підтримує використання розумних контрактів, так і програмно-апаратних платформ, на яких розміщується це програмне забезпечення.

12. Розробка пропозицій стосовно процесуальних особливостей розгляду в суді суперечок, пов'язаних з розумними контрактами.

Висновки.

Розумні контракти – прогресивна форма контрактів, що створює умови для реалізації на практиці багатьох переваг, що обумовлюється використанням технологій Інтернету речей.

Розумні контракти – інноваційна форма контрактів, укладення, виконання та припинення яких відбувається з використанням мережевих комп'ютерних програмних та/або програмно-апаратних засобів, що мають взаємозв'язок з фізичними або цифровими об'єктами, за участю або без участі людини, що вимагає проведення системних і комплексних правових досліджень в рамках цивільного, фінансового та інформаційного права.

З метою зменшення невизначеності та вартості впровадження правового регулювання використання розумних контрактів доцільно орієнтуватися на стратегію яка полягає в максимально можливому використанні правових механізмів традиційної системи права з необхідним удосконаленням або розвитком окремих правових положень. До створення нових правових конструкцій слід вдаватися тільки в тому випадку, коли в існуючому законодавстві не знаходиться навіть віддаленої аналогії.

Список використаних джерел:

1. Баранов А.А. Интернет : объект правоотношений и предмет регулирования : монография / А.А. Баранов. – К. : Ред. журн. “Право Украины”, 2013. – 144 с.
2. General Assembly UN. 2016. Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels. General Assembly Economic and Social Council. 29 February 2016.
3. ISOC. 2016. A policy framework for an open and trusted Internet. An approach for reinforcing trust in an open environment. Internet Society (ISOC), 22 June.
4. ISOC. 2016. Global Internet Report. The Economics of Building Trust Online: Preventing Data Breaches. Internet Society (ISOC).
5. Marc-David L.2018. “Questioning Centralized Organizations in a Time of Distributed Trust”. Journal of Management Inquiry 27(1): 40-44.
6. Yermack, David. “Corporate Governance and Blockchains.” ERN: Econometric Studies of Corporate Governance (Topic) (2015): n. pag.
7. Al-Turkistani, H. and N K. AlSa’awi. 2020. “Poster: Combination of Blockchains to Secure Smart Home Internet of Things.” 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH): 261-262.
8. Muhati, E, at el. 2022. “A New Cyber-Alliance of Artificial Intelligence, Internet of Things, Blockchain, and Edge Computing.” IEEE Internet of Things Magazine 5: 104-107.
9. Баранов О. 2016. “Інтернет речей” як правовий термін”. Юридична Україна, 5-6: 96-103.

10. Singh, Nirvikar. 2008. "Transaction costs, information technology and development." Indian Growth and Development Review 1.2: 212-236.
11. Білодід, І. К., et al. 2018. "Словник української мови Академічний тлумачний словник (1970–1980)."
12. Seidel M. 2018. “Questioning Centralized Organizations in a Time of Distributed Trust”. *Journal of Management Inquiry* 27.1: 40-44.
13. Coase, Ronald H. 1984."The new institutional economics." *ZEITSCHRIFT für die gesamte Staatswissenschaft/Journal of Institutional and Theoretical Economics* H. 1 (1984): 229-231.
14. Ménard, Claude, and Mary M. Shirley, eds. 2005. *Handbook of new institutional economics*, 9. Springer.
15. Mellen, Robert. 2017. "Critical review of “The Truth About Blockchain”. *Harvard Business Review.*
16. Espinel V. 2005. *Deep Shift. Technology Tipping Points and Societal Impact.* World Economic Forum Survey Report.
17. David Yermack. D. 2017. “ Corporate Governance and Blockchains”. *Review of Finance*, 21, 1: 7–31.
18. Tapscott D, Tapscott A. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio/Penguin, 2016.
19. Iansiti, Marco, and Karim R. Lakhani. 2017. "The truth about blockchain." *Harvard business review* 95.1: 118-127.
20. Kupriyanovsky, V. P., et al. 2017. “Digital supply chains and blockchain-based technologies in the sharing economy." *International Journal of Open Information Technologies* 5.8: 80-95.
21. Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." *Harvard business review* 95.1 (2017): 118-127.

22. Gupta, V. "A brief history of blockchain: Harvard Business Review, February 28, 2017." *Accessed November* 22 (2017): 2017.
23. Баранов О. 2017. “Інтернет речей (IoT): правові проблеми застосування розумних контрактів”. *Інформація і право*. 4(23): 26-40.
24. Szabo, Nick. 1996. "Smart contracts: building blocks for digital markets." *EXTROPY: The Journal of Transhumanist Thought, (16)* 18.2: 28.
25. De Filippi, Primavera, and Samer Hassan. 2018. "Blockchain technology as a regulatory technology: From code is law to law is code." *arXiv preprint arXiv:1801.02507* (2018).
26. Savelyev, A. I. 2016. "Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classical Contract Law." *Civil Law Bulletin* 16.3: 32-60.
27. Ivkushkin, K., and A.Vashkevich. 2017. "Horizons of Smart Contracts." *Open Systems. DBMS* 3: 44-45.
28. Stark, Josh. 2016. "How Close Are Smart Contracts to Impacting Real-World Law?, CoinDesk."
29. De Filippi, P., and S. Hassan. 2018. "Blockchain technology as a regulatory technology: From code is law to law is code." *arXiv preprint arXiv:1801.02507*.
30. Raskin, Max. 2016. "The law and legality of smart contracts." *Geo. L. Tech. Rev.* 1: 305.
31. Savron, Luca. 2019. "How blockchain technology could change our lives." *Ursidae: The Undergraduate Research Journal at the University of Northern Colorado* 8.1: 10.
32. Bulgakov, I. 2016. "Smart Contracts and Modern Contract Law." *URL: https://zakon.ru/blog/2016/8/12/umnye_kontrakty_i_sovremennoe_dogovornoe_pravo*.

33. Hourani, Sara. 2017. "Cross-border smart contracts: boosting international digital trade through trust and adequate remedies." : 118-119.
34. Al Khalil, Firas, et al. "A solution for the problems of translation and transparency in smart contracts." *Government Risk and Compliance Technology Centre. Report, available at: http://www. grctc. com/wp-content/uploads/2017/06/GRCTC-Smart-Contracts-White-Paper-2017. pdf (accessed 31st August, 2017)* (2017).
35. Mou, Lili, et al. 2015. "On end-to-end program generation from user intention by deep neural networks." *arXiv preprint arXiv:1510.07211*.
36. Panetta, K. 2017. "Why Blockchain's Smart Contracts Aren't Ready for the Business World." *URL: https://www. gartner. com/smarterwithgartner/whyblockchains-smart-contracts-arent-ready-for-the-business-world*.

Розділ ІІІ

СИМБІОЗ СОЦІАЛЬНОГО ПІДПРИЄМНИЦТВА ТА ТЕХНОЛОГІЙ ІОТ: ЮРИДИЧНИЙ АСПЕКТ ЧЕРЕЗ ПРИЗМУ ЄВРОІНТЕГРАЦІЇ

Правове регулювання підприємництва в Україні
Взаємозв'язок технологій ІОТ соціального капіталу та підприємництва
Використання ІОТ та соціальні цінності в ініціативах ЄС
Використання ІОТ технологій у різних сферах соціального підприємництва
Гармонізація понять соціального та інноваційного підприємництва

Правове регулювання підприємництва в Україні

Посилення громадянського суспільства в Україні та курс на євроінтеграцію сприяли активізації діяльності не тільки неурядових громадських організацій та об'єднань, але й поширенню соціального підприємництва як ще однієї форми громадянського самовираження. В свою чергу, розвиток технологій Інтернету речей (IoT) відкрив нові можливості для реалізації соціального підприємництва. Зазвичай, дані теми розвиваються паралельно одна одній. В цьому розділі ми пропонуємо зануритись у взаємозв'язок новітніх технологій та підприємництва заради соціально значимого результату. Для початку пропонуємо проаналізувати наявні нормативно-правові акти щодо підприємництва, адже вони є основою для розуміння процесу взаємодії ініціаторів підприємницької діяльності з іншими суб'єктами загалом.

Серед основних чинних нормативно-правових актів щодо підприємництва в Україні варто виділити: Господарський кодекс України, Цивільний кодекс України, Податковий кодекс України, Закон України «Про підприємництво», Закон України «Про розвиток та державну підтримку малого і середнього підприємництва в Україні», Закон України «Про дозвільну систему у сфері господарської діяльності», Закон України «Про господарські товариства», Закон України «Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань» тощо. В законодавстві України непередбачено термін «соціальне підприємництво», натомість, якщо звернутись до визначення підприємництва загалом, то варто звернути увагу на ознаку соціальної мети такої діяльності, яка зазначається в дефініції поруч з метою досягнення економічних результатів.

Відповідно до ст. 42 Господарського кодексу України, підприємництво - це самостійна, ініціативна, систематична, на власний ризик господарська діяльність, що здійснюється суб'єктами

господарювання (підприємцями) з метою досягнення економічних і *соціальних результатів* та одержання прибутку. Таким чином, навіть за відсутності прямого визначення терміну соціального підприємництва в законодавстві, можна зробити висновок, що «соціальні результати» є невід'ємною складовою підприємництва в розумінні законодавця.

Варто погодитись з думкою, що важливу роль у створенні та розвитку соціальних підприємств має відігравати держава. Зокрема, необхідно:

- розробити спеціальну законодавчу базу щодо соціального підприємництва;

- розробити відповідну програму розвитку з визначеними пріоритетами фінансового забезпечення;

- створити інструменти залучення бізнесу та громадських організацій до соціального підприємництва;

- створити сприятливі умови у сфері оподаткування [1, с. 17].

Звернемось, до прикладу, до положень закону України «Про основи соціальної захисту осіб з інвалідністю в Україні». Він чітко визначає, що громадські організації людей з інвалідністю «мають право здійснювати необхідну господарську діяльність без мети отримання прибутку, а також господарську та підприємницьку діяльність шляхом створення госпрозрахункових установ і організацій із статусом юридичної особи, а також підприємств, заснованих на колективній власності громадських об'єднань». Цей випадок можна розглядати як приклад соціального підприємства [2, с. 107].

Законодавство в Україні повинно включати в себе роз'яснення основних понять і механізмів функціонування соціальних підприємств, а також чіткі напрями правової політики щодо таких них, зокрема, в частині пільгових умов щодо сплати податків.

Пропонуємо звернути увагу на кілька перспективних напрямків та потреб у законотворенні щодо соціальних підприємств:

1. Уточнення дефініції соціального підприємства;

2. Розробка правового регулювання для визначення статусу соціального підприємства;

3. Створення гнучких правових умов для підтримки свободи зайняття такою діяльністю.

4. Забезпечення контролю за дотриманням законодавства.

Надзвичайно важливо розробити саме рамковий нормативно-правовий акт для забезпечення діяльності соціального підприємництва, оскільки вона повинна залишатися вільною від надмірного втручання держави. Також в акті важливо враховувати, що соціальні підприємства часто базуються на інноваціях.

В той же час, використання інновацій іноді потребує наявності певних правових норм, оскільки в деяких випадках таке використання може бути небезпечним. Наприклад, невиконання споживачем інструкцій щодо використання об'єкта інновації може призвести до небезпечних наслідків як для цієї особи, так і для інших членів суспільства. Правові норми можуть допомогти уберегти соціального підприємця та суспільство від цієї небезпеки. Саме так право може допомогти соціальному підприємництву розвиватися екологічно та з використанням технологій IoT.

Взаємозв'язок технологій IOT соціального капіталу та підприємництва

Технології Інтернету речей (далі – IoT) є тим інструментом, який допомагає оптимізувати вирішення поточних проблем в суспільстві за рахунок швидкої обробки великих масивів інформації та швидкого прийняття рішень, які відповідають поточній ситуації. Тож соціальні підприємці все частіше починають використовувати технології IoT для подолання соціальних проблем.

Для початку пропонуємо з'ясувати більш детально суть соціального підприємництва. Це підприємницька діяльність спрямована на інноваційну, суттєву та позитивну зміну у суспільстві.

В той час коли бізнесмени концентровані на створенні фінансового прибутку, соціальні підприємці займаються *збільшенням соціального капіталу* [3, с. 5].

Поняття соціального капіталу має міждисциплінарний характер. Організацією економічного співробітництва і розвитку було прийнято визначення поняття «соціальний капітал». Відтак, *соціальний капітал* тлумачиться як мережі з усталеними в них спільними нормами, цінностями та домовленостями, які сприяють співробітництву в цих мережах або серед груп таких мереж [4, с. 54].

З цього випливає, що залучення соціального капіталу сприяє економічному розвитку. Це є основою соціального підприємництва. Поряд з тим, економічний розвиток – це «структурна та інституційна перебудова економіки у відповідності до викликів перед суспільством, які в сьогоднішніх умовах спрямовані на підвищення виробництва промислової продукції, покращення надання послуг населенню та підвищення їхнього рівня добробуту шляхом широкого використання сучасних технологій та інновацій» [5, с. 73].

Отже, запровадження сучасних технологій та інновацій, в тому числі, у вигляді IoT безпосередньо реалізує мету створення соціального підприємства, а саме – формування соціального капіталу та створення передумови для економічного розвитку.

З вищенаведеного можна зробити висновок, що соціальне підприємництво, так само як і право, є інструментом вирішення певної проблеми, однак за рахунок економічного, а не юридичного механізму врегулювання. Серед проблем, які нині постають перед суспільством найбільш глобальною є перенасичення інформацією та ускладнення перевірки достовірності інформації, що знижує здатність вчасного реагування законодавця на динамічну зміну суспільних відносин.

Вирішення даної проблеми можливе, в тому числі, за рахунок зусиль соціальних підприємців, які можуть локалізувати цю проблему на меншій території. IoT як реалізація обов'язкової ознаки інноваційності соціального підприємства є тим інструментом, застосування якого робить можливим таку локалізацію.

Розглянемо на прикладі проблеми дезінформації, яка є досить поширеною з огляду на можливість розповсюдження інформації через Всесвітню мережу Інтернет. І вже існує позитивний досвід вирішення даної проблеми на локальному рівні. Так, в 2016 році в Лондоні було зареєстровано соціальне підприємство, яке створило платформу репутації в Інтернеті Right of Reply [6]. Вона дозволяє відновити контроль над своєю репутацією в Інтернеті, спираючись на запатентований пошук та технологію блокчейну. Дана платформа спрямована на забезпечення швидких, вчасних та юридично обґрунтованих рішень як для споживачів, так і для компаній задля своєчасного реагування на негативний або помилковий вміст щодо себе чи своєї організації.

Реалізація проекту стала можливою завдяки:

1. чіткому формуванню соціальної мети;
2. передачі частини доходу на благодійність;
3. використанню інноваційних технологій блокчейну.

Узагальнюючи, можна зробити висновок, що застосування технологій Інтернету речей передбачає ефективне подолання соціальних проблем, тобто формування певної соціальної цінності – задоволення нагальних потреб суспільства в ситуаціях, де більш звичні механізми взаємодії не працюють або працюють з мінімальною користю.

Використання IOT та соціальні цінності в ініціативах ЄС

Процес формування соціальної цінності при використанні технологій IoT, на нашу думку, може має більше перспектив саме в межах соціального підприємництва, оскільки поєднує в собі ознаку інноваційності та спільну мету – отримання позитивного соціально значущого результату. Втім, задля ефективного використання технологій IoT необхідно сформувати шляхи врегулювання поточних правовідносин, що можуть виникати у зв’язку з їх використанням. В

цьому сенсі роль права є беззаперечною, а ефективність його використання можемо прослідкувати на прикладі ЄС, який вчасно відслідковує тенденції цифрової трансформації та використовує їх задля розвитку багатьох сфер життєдіяльності людини, в тому числі соціальної.

Варто відмітити, що ЄС має ряд ініціатив, присвячених саме соціальному підприємництву. Серед них варто виокремити наступні:

1) Ініціатива Європейської комісії щодо соціального бізнесу була започаткована в 2011 році та спрямована на сприяння соціальному підприємництву в ЄС. Він включає низку заходів для підтримки соціальних підприємців, таких як покращення доступу до фінансування, забезпечення навчання та наставництва, а також підвищення обізнаності про соціальне підприємництво.

2) Європейський соціальний фонд забезпечує фінансування ініціатив, спрямованих на покращення можливостей працевлаштування, зменшення бідності та сприяння соціальній інтеграції. Його можна використовувати для підтримки ініціатив соціального підприємництва, в тому числі пов'язаних із прямим використанням технологій ШІ [7].

3) Європейський інвестиційний фонд надає фінансування та гарантії малим і середнім підприємствам, включаючи соціальні підприємства. Це сприяє соціальним підприємствам в отриманні фінансування, необхідне для відкриття та розвитку свого бізнесу.

Виходячи з положень цих актів, соціальне підприємництво можна визначити як підприємницьку діяльність, спрямована на інноваційну, суттєву та позитивну зміну у суспільстві. В той час коли класичне підприємництво спрямоване на досягненні фінансового прибутку, соціальні підприємці націлені на досягнення певної соціальної цінності.

Варто також відзначити, що в змісті Резолюції Європейського парламенту від 6 липня 2022 року щодо плану дій ЄС щодо соціальної економіки підкреслено ключову роль, яку нові технології та ШІ можуть відігравати у створенні робочих місць та розвитку та

розширенні соціальної економіки [8]. Окремої уваги приділено важливості розширення доступу до навчальних програм із цифрових навичок і передових технологій. Загалом, прийняття даної Резолюції особливо підкреслює заохочення цифрового переходу у соціальній економіці (через оподаткування, державні закупівлі та державну допомогу).

Як бачимо, йдеться про можливості для соціального підприємництва, в тому числі, інноваційність діяльності якого заохочується не лише на національному рівні, а й на загальноєвропейському рівні.

Європейська комісія також запустила ініціативу «Цифрові соціальні інновації», яка спрямована на підтримку соціальних підприємців, які використовують цифрові технології для вирішення соціальних проблем [9].

Дослідницька та інноваційна програма Європейського Союзу Horizon Europe зосереджена на ШІ для соціального блага, яка спрямована на підтримку дослідницьких та інноваційних проектів, котрі використовують ШІ для вирішення соціальних проблем [10].

Серед інших європейських ініціатив варто згадати AI4EU [11]. Це проект, що фінансується Європейською комісією і спрямований на сприяння розвитку та поширенню ШІ в Європі. Проект включає ряд ініціатив для підтримки використання ШІ в різних секторах, включаючи соціальне підприємництво.

У 2019 році Європейський альянс AI запустив ініціативу «AI for Good», щоб дослідити, як штучний інтелект можна використовувати для вирішення соціальних та екологічних проблем [12]. Це говорить про тенденції та місію, яка закладається у сам факт використання технологій Інтернету речей та штучного інтелекту.

Соціальна орієнтованість є надзвичайно цінним вектором, який задається демократичними державами, які поширюють гуманістичні ідеї. Новітні технології мають стати передумовою підвищення якості життя та запорукою благополуччя населення, а не причиною воєн, конфліктів та розбрату, яке неминуче призведе до

гибелі людства. Соціальне підприємництво має стати однією з поширених способів популяризації екологічного використання технологій IoT та ШІ. Саме держава за допомогою законотворення має закласти цей тренд.

У 2019 році Європейська комісія також випустила перелік етичних принципів для надійного штучного інтелекту [13]. Ці рекомендації забезпечують основу для розробки та розгортання штучного інтелекту прозорим, підзвітним і соціально відповідальним способом. Формування культури використання ШІ дозволить зробити дані технології, з одного боку, більш доступними для широких мас населення, а з іншого боку, створить зрозумілий та безпечний простір для використання ШІ.

Використання IOT технологій у різних сферах соціального підприємництва

Пропонуємо розглянути деякі приклади таких підприємств, які досягають соціально важливих результатів саме завдяки інноваційним технологіям. Серед них варто представити Good-Loop – соціальне підприємство, яке використовує технології ШІ для створення етичної реклами [14]. Їхня платформа дозволяє брендам рекламувати споживачів, а також підтримує соціальні та екологічні причини. Good-Loop використовує алгоритми штучного інтелекту, щоб персоналізувати рекламу та забезпечити її доставку споживачам, які, найімовірніше, зацікавляться нею.

Сфера енергетики потребує особливою уваги, особливо з огляду на кардинальну зміну підходів у зв'язку з російсько-українською війною. Наприклад, соціальне підприємство Enerbrain використовує технології штучного інтелекту для оптимізації енергоспоживання будівлі. Їхня платформа використовує датчики та алгоритми штучного інтелекту для моніторингу використання енергії

та визначення областей, де енергію можна заощадити, зменшуючи витрати та вплив на навколишнє середовище [15].

В умовах все більшого поширення штучного інтелекту виникатиме питання як впроваджувати ці технології в урбаністику. На прикладі Humanising Autonomy можна пересвідчитись у ефективності використання технологій ШІ для підвищення безпеки пішоходів. Їхня платформа використовує алгоритми ШІ для прогнозування поведінки пішоходів і попередження водіїв, допомагаючи запобігати аваріям і рятувати життя [16].

Вважаємо за доцільне піднімати питання забезпечення права на освіту завдяки новітнім технологіям. Наприклад, соціальне підприємство EIDU використовує освітні технології на основі ШІ, щоб забезпечити доступ до якісної освіти для дітей із малозабезпечених громад [17]. Їхня платформа надає студентам інтерактивні навчальні матеріали та персоналізовану підтримку, а також використовує алгоритми ШІ для відстеження прогресу та адаптації навчання до індивідуальних потреб.

IoT-технології є новою парадигмою, яка об'єднує безліч предметів навколо нас, спрощуючи життя людини. Ці технології поступово стають невід'ємною частиною нашого життя, особливо в період пандемії, коли слово «дистанційність» стає ключовою ознакою взаємодії в більшості сфер діяльності людини. Це стосується й освітнього процесу, адже навчальні заклади різних рівнів незалежно від форми власності чи напряму навчання в 2020 році вимушено перейшли на дистанційну форму навчання через вірусну загрозу у вигляді COVID-19. Згодом цей формат довелось продовжити через війну. Почали з'являтись так звані smart школи, тобто такі, що використовують IoT технології в своїй безпосередній роботі [18]. В більшості випадків вони стосуються розвитку популярного нині напряму STEM-освіти (S – science, T – technology, E – engineering, M – mathematics), в межах якої учням пропонується використання інноваційних технологій в процесі навчання.

Зазначимо, що Європейська Комісія досить активно зосередилась на питанні цифрової освіти. Наразі розроблено План дій щодо цифрової освіти (2021–2027), метою якого є сприяння розвитку високоефективної цифрової освітньої екосистеми [19]. Серед напрямів роботи в даному документі визначено розробку етичних стандартів використання штучного інтелекту (AI) та отриманих даних про студентів та викладачів в процесі навчанні.

Обсяги даних у формі матеріалів для навчання, балів, видів роботи навчального та наукового спрямування стали ще більшими, адже оффлайн форми комунікації з учнями та студентами перестали бути доступними. Виник ряд важливих питань щодо відкриття доступу до лекцій в режимі реального часу чітко визначеному колу осіб, їх ідентифікація, встановлення фактичної присутності особи на заході, а не суто технічного приєднання до заняття тощо.

Прикладами використання технологій Інтернету речей є наступні:

6. Аналіз даних веб-камер студентів за критеріями реальної відвідуваності дистанційного курсу, поведінковими показниками щодо концентрації на матеріалі, втраті уваги, ступеня перевтоми в процесі заняття, аналіз даних щодо емоційних станів, які також впливають на сприйняття інформації.

7. Аналіз звуків через певні інтервали часу, отриманих з мікрофону особи, що навчається також може бути проаналізовано за індикаторами мови, шуму, швидкості та інтенсивності натискання клавіш, чи було завдання, в якому студент мав задіяти клавіатуру тощо.

8. GPS-трекери, smart годинники можуть використовуватись для моніторингу місцезнаходження, фіксації та інтенсивності рухів особи, що навчається, тривалості фізичних вправ. Зібрання таких даних може застосовуватись при дистанційному навчанні дисциплін, пов’язаних зі спортивними навантаженнями. Окрім цього, такі дані, зокрема, швидкість серцебиття можуть бути корисними при прийнятті викладачем дистанційного іспиту, коли

досить складно повністю унеможливити використанням студентами додаткових джерел чи сторонньої допомоги [20, с. 1671-1672].

Таким чином, за допомогою технологій IoT та з використанням вищезгаданих технічних пристроїв стає можливим автоматичне фіксування та моніторинг присутності студентів на заняттях, аналіз паттернів поведінки, динаміки навчання, залучення в навчальний процес, ефективності тих чи інших завдань та способів донесення інформації тощо.

Оскільки в вищевказаному Плані дій ЄС щодо цифрової освіти на 2021-2027 роки передбачено використання даних учнів та викладачів, які фактично будуть користувачами технології штучного інтелекту та IoT, варто встановити чіткі межі між тим, які дані можуть використовуватися в освітній діяльності, а які можна вважати втручанням в приватне життя. На нашу думку, варто застосовувати принцип співмірності та виправданості використання певних даних про фактичного користувача здобутків цифрової трансформації в сфері освіти.

Жодним чином не можна допускати безальтернативності надання доступу до даних користувача освітньої послуги чи особи, яка таку послугу надає. Більше того, використання таких даних є недопустимим без надання згоди не тільки в технічному розумінні цього слова, наприклад, через згоду на умови роботи певного додатку. На нашу думку, установа, організація чи фізична особа, що надає освітню послугу має до угоди про надання послуги долучати також додаток, в якому передбачено виключний перелік технологій AI та IoT, які планується використовувати при навчанні, а також згода на обробку конкретних видів даних, як можуть бути отримані з мікрофону, відеокамери, GPS-навігатора тощо.

Специфіка освітньої діяльності в умовах пандемії, з одного боку, показала ще більшу необхідність застосування інноваційних технологій, а з іншого – вказала на потребу додаткового правового регулювання договірних відносин в цій сфері задля уникнення загроз конфіденційності та посягання на приватність. Цифрова

трансформація відкриває значні перспективи застосування технологій IoT в системі совіти, втім, мають бути забезпечені правила гри для такої взаємодії, що можливо через передбачення в законодавстві певних правових запобіжників зловживанню цифровими технологіями з боку суб'єктів освітнього процесу.

Таким чином, ШІ може допомогти подолати соціальні виклики більш інноваційним способом. Окрім цього, технології IoT та ШІ можуть сприяти соціальним підприємствам масштабувати свій вплив, автоматизуючи повторювані завдання та надаючи інформацію на основі даних, яка може стати основою для прийняття рішень. ШІ також може допомогти соціальним підприємствам краще зрозуміти своїх бенефіціарів і взаємодіяти з ними, аналізуючи дані про їхні потреби та вподобання.

Гармонізація понять соціального та інноваційного підприємництва

Тенденції безперечно говорять про те, що застосування технологій ШІ ставатиме дедалі більш масовим та буде сприяти подоланню різних викликів, які постають перед людством. З точки зору соціального підприємця застосування даних технологій має безперечні переваги. Законотворцям та юристам залишається продумати правила гри для подолання ризиків та супроводження використання технологій ШІ.

Хоч в національному законодавстві і відсутнє поняття соціального підприємства, втім, наявне визначення поняття «інноваційне підприємство». Відповідно до ст. 1 Закону України «Про інноваційну діяльність», таке підприємство (інноваційний центр, технопарк, технополіс, інноваційний бізнес-інкубатор тощо) визначено як - підприємство (об'єднання підприємств), що розробляє, виробляє і реалізує інноваційні продукти і (або) продукцію чи послуги, обсяг

яких у грошовому вимірі перевищує 70 відсотків його загального обсягу продукції і (або) послуг.

В розумінні даного закону інноваційним продуктом є результатом виконання інноваційного проекту і науково-дослідною і (або) дослідно-конструкторською розробкою нової технології (в тому числі - інформаційної) чи продукції з виготовленням експериментального зразка чи дослідної партії. Відповідно до ч. 2 ст. 14 Закону України «Про інноваційну діяльність», рішення про кваліфікування продукту інноваційним приймає центральний орган виконавчої влади, що реалізує державну політику у сфері інноваційної діяльності, за результатами експертизи [21].

Така є процедура визнання передбачена щодо інноваційної продукції. З огляду на викладені в законі вимоги, можна дійти висновку, що в державі наявна процедура визнання підприємства інноваційним, а отже розробка, вироблення та реалізація інноваційних продуктів і (або) продукції чи послуги, зокрема, з використання технологій IoT виокремлює інноваційне підприємство в окрему категорію. Втім, питання визнання такого підприємства соціальним залишається виключно на розсуд його засновників і не тягне за собою правових наслідків.

Отже, технології IoT та ШІ допомагають оптимізувати вирішення поточних проблем в суспільстві за рахунок швидкої обробки великих масивів інформації та швидкого прийняття рішень, які відповідають поточній ситуації. Тож соціальні підприємці все частіше починають використовувати дані технології для подолання соціальних викликів та досягнення соціально значимого результату. Завданням законотворця залишається створити сприятливі умови для такої діяльності, зокрема, у формі соціального підприємництва із залученням інноваційних рішень та технологій, враховуючи досвід ЄС у цій сфері.

Список використаних джерел:

1. Голуб'як Н. Р. Соціальне підприємництво як механізм вирішення соціально-політичних проблем. S.P.A.C.E. Society, Politics, Administration in Central Europe: електронний науково-практичний журнал / редкол.: Д. В. Яковлев (голов. ред.), К. М. Вітман (заст. голов. ред.), Д. Ю. Дворніченко (відп. секр.) [та ін.]; НУ «ОЮА». Одеса, 2017. Вип. 2. С. 16-20.
2. Давидовська Г. Проблеми соціального підприємництва в Україні. Науковий вісник УжНУ. 2016. № 7 (1). С. 106–109.
3. Долуда Л., Назарук В., Кірсанова Ю. Соціальне підприємництво. Бізнес-модель. Реєстрація. Оподаткування. Київ: ТОВ «Агентство «Україна». 2017. 92 с.
4. Шаповалова Т. В. Соціальний капітал: теоретичні засади та стратегії трансформації: монографія. Східноукр. нац. ун-т ім. Володимира Даля. Сєвєродонецьк: Вид-во СНУ ім. В. Даля, 2016. 359 с.
5. Creating a favourable climate for social enterprises, key stakeholders in the social economy and innovation. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?
uri=COM:2011:0682:FIN:EN:PDF (дата звернення: 15.06.2023).
6. Right of reply. URL: https://rightofreply.news/ (дата звернення: 26.04.2023).
European Social Fund Plus. URL: https://ec.europa.eu/european-social-fund-plus/en (дата звернення: 20.04.2023).
7. European Social Fund Plus. URL: https://ec.europa.eu/european-social-fund-plus/en (дата звернення: 20.04.2023).
8. European Parliament resolution of 6 July 2022 on the EU action plan for the social economy. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0288_EN.html (дата звернення: 17.08.2023).
9. Digital Social Innovation for Europe. URL: https://cordis.europa.eu/project/id/688192 (дата звернення: 15.08.2023).

10. Horizon Europe. URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en (дата звернення: 17.06.2023).
11. The AI4EU consortium. URL: https://www.ai4europe.eu/about-ai4eu (дата звернення: 05.05.2023).
12. AI for good. URL: https://www.aiforgood.eu/ (дата звернення: 12.07.2023).
13. Ethics guidelines for trustworthy AI. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (дата звернення: 17.08.2023).
14. Good-Loop. URL: https://good-loop.com/ (дата звернення: 19.03.2023).
15. Enerbrain. URL: https://www.enerbrain.com/ (дата звернення: 05.02.2023).
16. Humanising Autonomy. URL: https://humanisingautonomy.com/ (дата звернення: 17.08.2023).
17. The EIDU platform. URL: https://eidu.com/ (дата звернення: 02.08.2023).
18. Kusmin, M.; Saar, M.; Laanpere, M. Smart schoolhouse – Designing IoT study kits for project-based learning in STEM subjects. In Proceedings of the Global Engineering Education Conference (EDUCON), Tenerife, Spain, 17–20 April 2018; pp. 1514-1517.
19. Резолюція Digital Education Action Plan (2021-2027). URL: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en (дата звернення: 09.04.2023).
20. Ilieva, Galina; Yankova, Tania. IoT in Distance Learning during the COVID-19 Pandemic. TEM Journal. Volume 9, Issue 4. pp. 1669-1674.
21. Про інноваційну діяльність. URL: https://zakon.rada.gov.ua/laws/show/40-15#Text (дата звернення: 03.04.2023).

Розділ IV

ПРАВОВЕ РЕГУЛЮВАННЯ ДАНИХ В ЄС: ПОДОЛАННЯ ВИКЛИКІВ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ РОЗБУДОВИ ЕКОНОМІКИ ДАНИХ

Взаємозв'язок економіки даних та Інтернету Речей.
Правове регулювання економіки даних в ЄС.
Вирішення проблеми локалізації даних для функціонування економіки даних.
Роль відкритих даних в екосистемі Інтернету речей.
Роль дослідницьких даних для розбудови технологій IOT.
Правове регулювання цифрового контенту і послуг в ЄС.
Роль конкурентних ринків у цифровому секторі.
Захист персональних даних в екосистемі цифрових платформ Інтернету Речей.
Гармонізація норм про надання цифрових послуг.
Регулювання цифрової економіки в ЄС згідно з DMA, DSA та GDPR.
10 сфер впливу DSA та GDPR на обробку даних.

Взаємозв'язок економіки даних та Інтернету Речей

Інформаційно-комунікаційні технології більше не є окремим сектором, вони є основою всіх сучасних інноваційних економічних систем і суспільств. Електронні дані знаходяться в центрі цих систем і можуть принести велику цінність, якщо їх проаналізувати або поєднати з послугами та продуктами. У той же час швидкий розвиток економіки даних і нових технологій, таких як штучний інтелект, продукти та послуги Інтернету речей, автономні системи та 5G, породжують нові правові проблеми, пов'язані з питаннями доступу та повторного використання даних, відповідальності, етики.

Ланцюжки вартості даних побудовані на різних видах діяльності з даними: створення та збір даних; агрегація та організація даних; обробка даних; аналіз даних, маркетинг і розповсюдження; використання та повторне використання даних [6].

Саме тому набуває актуальності розробка правового забезпечення нормативних актів, які встановлюють правові режими обробки для різних сфер різних наборів даних.

Цифрові технології змінюють економіку та повсякденне життя людей у всьому світі. Дані стали надважливим ресурсом для економічного розвитку: вони є основою для багатьох нових продуктів і послуг.

Враховуючи, що дані накопичуються та використовуються у великих обсягах, до таких масивів неструктурованих даних є інтерес у комерційних компаній виникла необхідність правового регулювання даних.

У традиційній моделі економіки, показником "успішності" бізнесу був розмір компанії (капітал, активи, прибутки, кількість співробітників, асортимент товару тощо), у новій економіці, де виробництво орієнтоване на послуги і операції з нематеріальними активами, основним критерієм успіху є здатність компанії управляти своєю продуктивністю і ефективністю, а головним засобом виробництва є корпоративні знання.

У зв'язку із стрімким розвитком інформаційно-комунікаційних технологій змінилась світова кон'юктура ринку. Характер споживання послуг зазнав кардинальних змін. Споживач очікує задоволення його запитів 24\7, і багато в чому, саме він формує запит до представників бізнесу в частині створення персоналізованого товару, робіт і послуг. Збільшення потреб споживачів, вимагає значної гнучкості бізнес-процесів. Ці процеси одночасно мають сприяти як задоволенню зростаючих потреб споживачів, так і підвищувати рівень конкурентоспроможності [1, с. 80].

Процес цифровізації в економіці вплинув на розвиток учасників господарських відносин. Етапами формування цифрової економіки є:

- цифровізація бізнесу,
- цифрова трансформація бізнесу,
- цифрова економіка,
- економіка результату.

Цифровізація бізнесу – це кардинальна зміна парадигми усіх бізнес-процесів, зокрема, схем виробництва, постачання і продажу товарів, інтерактивної взаємодії та маркетингові стратегії та інших процесів, шляхом їх реалізації за допомогою цифрових технологій [1, с.82].

Цифрова трансформація бізнесу – це зміна всіх бізнес-процесів: від місії компанії до процесу постачання послуг, яка повністю здійснюється на базі цифрових технологій [1, с.82].

Цифрова економіка – це система суспільних відносин, які формуються у зв'язку із потребою споживача в задоволенні його інтересів, де формування попиту і пропозиції, надання послуг, доставка товарів здійснюється учасниками господарських відносин з використанням цифрових платформ [1, с.81]

Цифрова платформа – веб-сайт, який забезпечує інформаційну взаємодію між споживачем та бізнесом, і охоплює усі етапи надання послуги чи отримання товару з використанням мережі Інтернет [1, с.82]

Економіка результату – це ресурсозберігальна, функціонально таргетована економічна діяльність суб'єктів масового ринку щодо задоволення індивідуальних прав, інтересів та потреб будь-якого конкретного споживача з можливістю динамічного формування ситуативної кооперації для функціональної взаємодії з будь-якими іншими суб'єктами ринку на основі використання глобальної мережі Інтернету речей [2, с. 232].

Традиційні інститути інформаційного права включали правове регулювання "право на інформацію", "свободи слова", "інститут таємниць" (державної, адвокатської, банківської, лікарської, усиновлення, сповіді та інші), "конфіденційності інформації", "персональних даних".

У зв'язку із появою великої кількості пристроїв, під'єднаних до мереж Інтернет, цифрової трансформації бізнесу, появи цифрових екосистем обороту даних та нового тику суспільних відносин виникла необхідність в правовому регулюванні інших категорій даних.

Економіка даних – це форма реалізації суспільних відносин в цифровій економіці шляхом створення, збору, зберігання, обробки, розповсюдження, аналізу, опрацювання, передачі та використання даних, які є основним предметом суспільного інтересу.

В економіці даних використовуються як персональні дані, так і промислові (індустріальні) набори неособистих даних, відкритих даних, метаданих, Великих даних. Для розвитку економіки даних в Україні важливо визначити правові режими всіх категорій даних, які можуть бути використані у процесах машинного навчання та інших технологій розвитку штучного інтелекту [3, с. 72].

В Європейському союзі є такі Регламенти і Директиви, які системно започаткували правове регулювання різних типів даних. Деякі з цих директив сформували основи для майбутнього розвитку економіки даних. Звичайно, передбачити всі правові виклики обробки даних не було можливості. Тому частина частина Регламентів і Директив була ухвалена як відповідь на виклики і проблеми, які

виникли у зв'язку із розбудовою економіки даних технологій Інтернету Речей та економіки результату.

Правове регулювання економіки даних в ЄС

У даному розділі будуть коротко представлені найбільш впливові документи, які вплинули на становлення і розвиток економіки даних.

2016 рік — Загальний регламент про захист даних (GDPR) [4].
2018 рік — Регламент про вільний рух неперсональних даних [5].
2019 рік — Директива про відкриті дані [6].
Директива про цифровий контент [7].
2020 — Регламент про управління даними (DGA) [8].
2022 — Регламент про цифрові послуги (DSA) [9].
Регламент про цифрові ринки (DMA) [10].

Звичайно, що це не повний перелік актів, який формує систему правового регулювання економіки даних, ми прагнули назвати основні акти, хоча велике значення для системи правового регулювання мають також:

Регламент про конкурентні та чесні ринки в цифровому секторі [11]

Директива про нерозкрите ноу-хау та бізнес-інформацію [12],

Регламент про кібербезпеку (CSA) [13],

Директива про електронну комерцію [14],

Регламент про цифрову операційну стійкість (EU) 2022/2554 (DORA) [15].

Положення Директиви щодо захисту нерозкритого ноу-хау та бізнесової інформації (комерційної таємниці) проти їх неправомірного набуття, використання та розкриття чітко передбачають, що комерційна таємниця не є об'єктом права інтелектуальної власності. Тому створена система правової охорони об'єктів інтелектуальної

власності не може забезпечити такі ж правові гарантії для особливого виду інформації – комерційної таємниці і ноу-хау [16, с. 125].

Важливість цього положення впливає також на захист наборів даних, та алгоритмів обробки, оскільки, можуть становити комерційну цінність для суб'єктів економіки даних. Окреме значення має правове регулювання кібербезпеки, оскільки норми цього акту безпосередньо визначають механізми правового захисту.

Директива про електронну комерцію закладала основи для формування вільного руху послуг інформаційного суспільства між державами-членами забезпечення правової визначеності та довіри споживачів ця Директива повинна встановлювати чітку та загальну структуру для охоплення певних правових аспектів електронної комерції на внутрішньому ринку [14].

Вирішення проблеми локалізації даних для функціонування економіки даних

Локалізація даних - означає будь-які зобов'язання, заборони, умови, обмеження чи інші вимоги, передбачені законами, нормативними або адміністративними положеннями або випливають із загальної та послідовної адміністративної практики в державі-члені та в органах, що регулюються публічним правом що перешкоджає обробці даних у будь-якій іншій державі-члені [6, ст. 3].

Національне правове регулювання часто вимагає розміщення серверів, де здійснюється обробка даних у межах юрисдикції країни, особливо, якщо здійснюється обробка персональних даних. Разом з цим, існують вимоги, щодо використання технологічних засобів, сертифікованих або схвалених у певній державі-члені країн ЄС.

Правова невизначеність щодо обсягу законних і нелегітимних вимог щодо локалізації даних ще більше обмежує вибір, доступний гравцям ринку та державному сектору щодо місця обробки даних [6, п.4].Також існує проблема перенесення наборів даних до різних технологічних платформ їх обробки, наприклад у зв'язку із

завершенням послуг хостингу, чи зміни оператора хмарних сервісів, чи масштабування бізнес процесів, що вимагає збільшення обчислювальних потужностей.

Отже, прийняття єдиних правил для:

- зменшення розбіжностей між національними законами;
- формування єдиних правових режимів торгівлі (обміну даними);
- уникнення ситуації надмірної невиправданої конкуренції - є актуальним завданням.

Для правового регулювання обробки і транскордонного переміщення персональних даних існують норми GDPR. Якщо технологічний розвиток створює можливості для перетворення анонімних даних на персональні, то їх охорона і опрацювання здійснюється у відповідності до норм Регламенту. Проблемою є те, що GDPR не накладає зобов'язання зберігати різні типи даних окремо. У зв'язку із цим в наборах неперсональних даних може бути частина персональних. Або через виконання алгоритмічних процедур з набору неперсональних даних можна легко отримати персональні. І таким чином, без належного захисту залишається набір неперсональних даних на етапі його переміщення і обробки, що створює правову невизначеність та простір до зловживань.

При розробці правового регулювання має бути дотримано баланс між мінливими потребами користувачів, постачальників послуг і збігів механізмів правового регулювання з існуючими актами держав-членів Союзу. Складність дотримання такого балансу полягає у тому, щоб запропонувати гнучкі ефективні механізми, які ні в технічному, ні в правовому, ні в організаційному плані не повинні обтяжити виконання цих норм учасниками Союзу. Саме такий підхід дозволяє сформувати співпрацю між країнами та забезпечити принцип саморегулювання.

Директива [6] застосовується до обробки даних у найширшому сенсі, охоплюючи використання всіх типів IT-систем, незалежно від

того, чи розташовані вони на території користувача, чи передані постачальнику хмарних послуг, наприклад
зберігання даних на фізичному сервері

- на умовах хмарного рішення “інфраструктура як послуга (IaaS)
- обробки даних на платформах з власною IT- інфраструктурою чи відповідного хмарного рішення “платформа як послуга” (PaaS))
- безпосередня обробка даних в ліцензованих програмах чи хмарному рішенні - на умовах надання програмного забезпечення — як послуги (SaaS) [6, п.17].

Для подолання правових бар’єрів норми Регламенту зобов’язують:

- надсилати Комісії проекти актів, що встановлюють вимоги до локалізації даних [6, п. 21].
- прийняття нових вимог правового регулювання щодо локалізації актів можуть бути ухвалені з підстав забезпечення національної безпеки, але такі заходи мають бути співмірними із поставленою метою та не виходити за їх межі [6, п.19].

Вимоги до локалізації даних часто виникають через відсутність довіри до транскордонної обробки даних.

Існує ризик недоступності даних для цілей компетентних органів держав-членів, наприклад, для перевірки та аудиту для регулятивного чи наглядового контролю. Ефективним механізмом подолання цієї проблеми є встановлення функціональних вимог для опису систем де зберігаються дані, щоб мати доступ для реалізації цілей державних органів.

Для вирішення проблеми конкуренції провайдерів послуг норми Регламенту встановлюють м’яке право у формі Кодексів поведінки провайдерів, які самостійно визначають та інформують споживачів про:

- окремі компоненти різноманітних послуг обробки даних;
- положення договорів про перенесення даних при розірванні договору;

- детальну інформацію та операційні вимоги до перенесення даних [6, п.30].

Такі кодекси поведінки мають охоплювати ключові аспекти для перенесення даних:

- розташування резервних копій даних;
- доступні формати даних і підтримку;
- необхідна IT-конфігурація та мінімальна пропускна здатність мережі;
- час, необхідний для початку процесу перенесення,
- час, протягом якого дані залишатимуться доступними для перенесення;
- гарантії доступу до даних у разі банкрутства постачальника послуг;
- блокування постачальників є неприйнятною діловою практикою [6, п.31].
- Підходи до схем сертифікації, які полегшують порівняння продуктів і послуг обробки даних для професійних користувачів.

Такі підходи можуть включати:

- управління якістю,
- управління інформаційною безпекою,
- управління безперервністю бізнесу
- управління навколишнім середовищем.

Проблемним аспектом залишається сфера обробки комбінованого набору даних, оскільки Директива [6] застосовується до частини набору даних, що не стосується персональних даних. Якщо персональні та неособисті дані в наборі даних нерозривно пов'язані, цей Регламент не перешкоджає застосуванню норм GDPR, фактично надаючи пріоритет нормам про захист персональних даних.

Враховуючи великі обсяги даних, які обробляють органи державної влади, залучаючи провайдерів і постачальників послуг обробки даних, органи державної влади мають утримувалися від встановлення обмежень щодо локалізації даних, адже такий підхід

підвищить конкурентоспроможність постачальників послуг з різних країн Союзу і тому забезпечить зростання інновацій [6, п.13]

Роль відкритих даних в екосистемі Інтернету речей

Директива про відкриті дані та повторне використання даних державних органів мала важливе значення для встановлення правового регулювання доступу та комерційного використання вже створених даних.

Державний сектор збирає, виробляє, відтворює та поширює широкий спектр інформації в багатьох сферах діяльності, таких як соціальна, політична, економічна, юридична, географічна, екологічна, метеорологічна, сейсмічна, туристична, бізнес, патентна та освітні галузі. Документи, створені органами виконавчої, законодавчої чи судової влади державного сектору, становлять величезний, різноманітний і цінний фонд ресурсів, які можуть принести користь суспільству. Надання цієї інформації, яка включає динамічні дані, у загальновживаному електронному форматі дозволяє громадянам і юридичним особам знаходити нові способи їх використання та створювати нові, інноваційні продукти та послуги.

Інтелектуальне використання даних, включаючи їх обробку за допомогою додатків штучного інтелекту, може мати трансформаційний вплив на всі сектори економіки [6, п.8].

Ця Директива встановлює ряд важливих визначень для наборів даних. Зокрема:

Динамічні дані означають документи в цифровій формі, що підлягають частому оновленню або оновленню в режимі реального часу, зокрема через їхню мінливість або швидке старіння; дані, створені датчиками, зазвичай вважаються динамічними даними.

Дослідницькі дані означають документи в цифровій формі, крім наукових публікацій, які збираються або виготовляються в ході науково-дослідницької діяльності; використовуються як докази в дослідницькому процесі, або загальноприйняті дослідницьким

співтовариством як необхідні для підтвердження висновків та результатів досліджень.

Високоцінні набори даних означають документи, повторне використання яких пов'язане з важливими перевагами для суспільства, навколишнього середовища та економіки, зокрема через їхню придатність для створення додаткових послуг, додатків, нових робочих місць.

Машиночитатний формат означає формат файлу, структурований таким чином, що програми можуть легко ідентифікувати, розпізнавати та витягувати конкретні дані, включаючи окремі твердження фактів, та їхню внутрішню структуру.

Відкритий формат означає формат файлу, який не залежить від платформи та доступний для громадськості без будь-яких обмежень, які перешкоджають повторному використанню документів [6].

Повторне використання включає використання документів за межами суспільних завдань, які було створено чи отримано державним сектором для надання послуг у загальних інтересах у самій організації для діяльності [6, п. 20].

З моменту прийняття першого набору правил щодо повторного використання інформації державного сектору кількість даних у світі, включно з загальнодоступними, зросла в геометричній прогресії. Паралельно відбувається постійний розвиток технологій для аналізу, використання та обробки даних, таких як машинне навчання, штучний інтелект та Інтернет речей. Ця швидка технологічна еволюція робить можливим створення нових послуг і нових програм, які побудовані на використанні, агрегації або комбінації даних [6, п.10].

Еволюція суспільства, заснованого на даних, де використовуються дані з різних сфер і видів діяльності, впливає на життя кожного громадянина в Союзі, зокрема, надаючи їм змогу отримати нові способи доступу до знань і їх отримання [6, п.11].

Цифровий контент відіграє важливу роль у цій еволюції. Протягом останніх років виробництво контенту сприяло швидкому створенню робочих місць і продовжує це робити [6, п.12].

Інформація державного сектору або інформація, зібрана, створена, відтворена та поширена в рамках виконання суспільного завдання або послуги загального інтересу, є важливим первинним матеріалом для продуктів і послуг цифрового контенту та стане ще більш важливим ресурсом, з розвитком передових цифрових технологій, таких як штучний інтелект, технології розподіленої реєстру (блокчейн) та Інтернет речей [6, п.13].

Політика відкритих даних, яка заохочує широку доступність і повторне використання інформації державного сектору в приватних або комерційних цілях, з мінімальними правовими, технічними чи фінансовими обмеженнями або без них, і які сприяють обігові інформації не тільки для суб'єктів господарювання, але в першу чергу для громадськості, може відігравати важливу роль у сприянні соціальному залученню, а також дати поштовх і сприяти розвитку нових послуг на основі нових способів поєднання та використання такої інформації [6, п.16].

Роль дослідницьких даних для розбудови технологій ІОТ

Обсяг отриманих дослідницьких даних зростає в геометричній прогресії та має потенціал для повторного використання за межами наукової спільноти. Для того, щоб мати можливість ефективно та цілісно вирішувати зростаючі суспільні проблеми, надзвичайно важливим є можливість доступу, поєднання та повторного використання даних із різних джерел, а також із різних секторів та дисциплін.

Дослідницькі дані включають статистичні дані, результати експериментів, вимірювань, спостереження в результаті польових робіт, результати опитувань, записи інтерв'ю та зображення, метадані, специфікації та інші цифрові об'єкти.

Відкритий доступ розуміється як практика безкоштовного надання кінцевому користувачеві онлайн-доступу до результатів

досліджень без обмежень щодо використання та повторного використання, окрім можливості вимагати підтвердження авторства.

Дослідницькі дані відрізняються від наукових статей, у яких повідомляються та коментуються висновки, отримані в результаті їх наукових досліджень.

Політика відкритого доступу спрямована, зокрема, на надання дослідникам і широкій громадськості доступу до дослідницьких даних якомога раніше в процесі розповсюдження та полегшення їх повторного використання. Відкритий доступ допомагає:

- підвищити якість,
- зменшити потребу в непотрібному дублюванні досліджень,
- пришвидшити науковий прогрес,
- боротися з науковим шахрайством,
- сприяє економічному зростанню та інноваціям.

Крім відкритого доступу, докладаються зусилля щодо управління даними, у вигляді стандартної наукової практики, для розповсюдження дослідницьких даних, які можна отримати та використати повторно, оскільки вони сумісні між собою [6, п.27].

Термін **«документ»** повинен охоплювати будь-яке представлення дій, фактів або інформації — і будь-яку компіляцію таких дій, фактів або інформації — незалежно від її носія (паперова чи електронна форма або як звуковий, візуальний чи аудіовізуальний запис). Визначення «документа» не стосується комп'ютерних програм [6, п. 30].

Документи також мають бути доступні для повторного використання після запиту, поданого повторним користувачем. У таких випадках ліміт часу для відповіді на запити щодо повторного використання має бути розумним і відповідати еквівалентному часу для запитів на доступ до документа за відповідними режимами доступу.

Проте державні підприємства, навчальні заклади, дослідницькі організації та організації, що фінансують дослідження, повинні бути звільнені від цієї вимоги. Розумні часові обмеження в усьому Союзі

стимулюватимуть створення нових агрегованих інформаційних продуктів і послуг на загальносоюзному рівні. Це особливо важливо для динамічних даних (включаючи дані про навколишнє середовище, дорожній рух, супутникові, метеорологічні та згенеровані датчиками дані), економічна цінність яких залежить від негайної доступності інформації та регулярного оновлення.

Таким чином, динамічні дані повинні бути доступні відразу після збору або у випадку оновлення вручну відразу після модифікації набору даних через інтерфейс прикладного програмування (API), щоб полегшити розробку мобільних і хмарних додатків на основі таких даних [6, п.31].

API — це набір функцій, процедур, визначень і протоколів для міжмашинного зв'язку та безперебійного обміну даними. API має підтримуватися чіткою технічною документацією, яка є повною та доступною в Інтернеті. Слід використовувати відкриті API або застосовувати стандартні протоколи та міжнародно визнані стандарти для наборів даних. API можуть мати різні рівні складності та означати просте посилання на базу даних для отримання певних наборів даних, веб-інтерфейс або більш складні налаштування.

Загальна цінність повторного використання та обміну даними за допомогою належного використання API:

допомагає розробникам і стартапам створювати нові послуги та продукти;

створення цінних екосистем навколо ресурсів даних, які часто не використовуються.

Налаштування та використання API має ґрунтуватися на кількох принципах:

- X доступність,
- X стабільність,
- X обслуговування протягом життєвого циклу,
- X однаковість використання та стандартів,
- X зручність для користувача,
- X безпека.

Можливості для повторного використання можна покращити, обмеживши потребу в оцифровуванні паперових документів або в обробці цифрових файлів, щоб зробити їх сумісними. Таким чином, органи державного сектору повинні робити документи доступними в будь-якому попередньо існуючому форматі [6, п.33].

Наприклад, опубліковані на веб-сайтах, доступними у відкритому та машинозчитуваному форматі разом із їхніми метаданими з високим рівнем точності та деталізації.

Дослідницькі дані часто отримуються за результатом реалізації спільних проектів. Між університетськими бібліотеками, музеями, архівами та приватними партнерами, можуть укладатись численні домовленості про співпрацю, які передбачають оцифрування культурних ресурсів із наданням ексклюзивних прав приватним партнерам. Ці колекції культурної спадщини та відповідні метадані є потенційною основою для продуктів і послуг цифрового контенту та мають величезний потенціал для інноваційного повторного використання в таких секторах, як навчання та туризм [6, п. 65].

Державно-приватні партнерства можуть сприяти корисному використанню культурних колекцій і водночас прискорювати доступ до культурної спадщини для представників громадськості.

Приватному партнеру може знадобитись виключне право на оцифровані культурні ресурси, для повернення своїх інвестицій. Цей період, однак, має бути обмежений найкоротшим часом, для забезпечення принципу доступності суспільного надбання.

Термін дії виключного права на оцифровані культурні ресурси, не повинен перевищувати 10 років. Будь-який період ексклюзивності, який перевищує 10 років, повинен підлягати перегляду, беручи до уваги технологічні, фінансові та адміністративні зміни в середовищі з моменту укладення угоди з приватними партнерами [6, п.49].

Правове регулювання цифрового контенту і послуг в ЄС.

Багато споживачів стикаються з проблемами, пов'язаними з якістю або доступом до цифрового контенту чи цифрових послуг. Споживачі не завжди впевнені у закордонних покупках, особливо, якщо вони здійснені онлайн. Одним із головних факторів відсутності довіри споживачів є невизначеність щодо їхніх ключових прав і відсутність чіткої договірної бази для цифрового контенту чи цифрових послуг [7,п. 5].

Для вирішення цієї проблеми необхідно:

1. гармонізувати норми споживчого договірного права в усіх державах-членах ЄС;
2. стабільне договірне середовище при постачанні цифрового контенту чи цифрових послуг в інших державах-членах;
3. зменшення правової фрагментації [7, п. 7].

Основні концептуальні підходи до вирішення зазначених проблем описані в Директиві про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг №2019/770 від 20 травня 2019 року (далі Директива 2019/770).

Положення цієї Директиви визначає, що споживачі повинні мати право на гармонізовані права на постачання цифрового контенту та цифрових послуг для задоволення потреб, зумовлених швидким технологічним розвитком комп'ютерних програм, відеофайлів, аудіофайлів, музичних файлів, цифрових ігор, електронних книг та інших електронних публікацій, а також цифрові послуги, які дозволяють створювати, обробляти, отримувати доступ або зберігати дані в цифровій формі, включаючи програмне забезпечення як послугу, наприклад, обмін відео та аудіо та іншими файлами, хостинг, обробка текстів, ігри, які пропонуються в середовищі хмарних обчислень і соціальних мережах [7,п. 19].

Існують різноманітні способи надання цифрового контенту або цифрових послуг та їх оплати. Наприклад: передача на матеріальному

носії DVD, CD, USB-накопичувачі і карти пам'яті, завантаження споживачами на свої пристрої, потокова передача в Інтернеті, надання доступу до можливостей зберігання цифрового контенту або доступ до використання соціальних медіа, застосовуватися до цифрового контенту [7, п. 19].

Диференціація залежно від методів оплати може включати цифрові представлення вартості, такі як електронні ваучери або електронні купони, вони можуть бути причиною дискримінації та створити невиправданий стимул для компаній у наданні контенту за нетрадиційну плату [7,п. 23].

Такою платою можуть бути не фіатні кошти чи цифрові представлення вартості, а особисті дані споживача.

Таким чином, правове регулювання має застосовуватися до контрактів, за якими продавець надає або зобов'язується надавати цифровий контент або цифрову послугу споживачеві, а споживач надає або зобов'язується надати свої персональні дані.

Наприклад, якщо споживач хоче отримати обліковий запис у соціальних мережах і надає ім'я та адресу електронної пошти, які використовуються для інших цілей ніж доступ до облікового запису соціальної мережі [7, п. 24], це може вважати угодою з нетрадиційним способом оплати послуг (фактично продаж персональних даних).

За загальним правилом, умови надання цифрового контенту мають узгоджуватись між продавцем і споживачем у договорі. Наприклад:

1. Зазначення опису, кількості файлів до яких можна отримати доступ, якості (наприклад, роздільна здатність зображення), мова та версія, умови про безпеку, функціональність, сумісність, можливості взаємодії та інші характеристики [7, п.42],наприклад, надання оновлень у спосіб, передбачений у договорі [7, п.44], якщо використання контенту обмежено у часі, має бути зобов'язання щодо надання оновлень у цей же час [7, п.47].

2. Споживач має залишатися вільним у виборі, чи встановлювати надані оновлення [7, п.47], при цьому встановлення чи

відмова від оновлення не має перешкоджати отриманню послуги та впливати на її функціонал.

3. Продавець повинен повідомити споживача про те, що рішення споживача не встановлювати оновлення, необхідні для підтримки відповідності цифрового вмісту або цифрової послуги, включаючи оновлення безпеки,

ступінь відповідності за загальним типом послуг, якість та безперервність надання послуги, наприклад хмарного сервісу [7, п.51].

4. Умови щодо сумісності, які передбачають, що цифровий контент і послуга мають бути правильно інтегровані в апаратне та програмне середовище споживача [7, п.52].

5. Обмеження щодо ліцензійної угоди кінцевого споживача. Продавець має повідомити про всі обтяження правами інтелектуальної власності контенту або послуги, якщо такі є. А споживач повинен мати можливість окремо погодитись з такою умовою договору.

6. Умови відповідальності продавця за неналежне надання цифрової послуги чи контенту [7, п.55] та визначення мінімального періоду, коли продавець має усунути недоліки доступу [7, п.56].

7. Умови поставки контенту можуть визначатись за такими моделями надання послуг:

- одноразово,
- період часу,
- безперервний спосіб доступу до послуги.

Після усунення недоліків доступу послуга має надаватись невідкладно, без невиправданої затримки [7, п.61].

8. Право односторонньої відмови чи розірвання договору споживачем у разі неусунення недоліків.

9. Право продавця вибрати спосіб усунення недоліків - шляхом випуску оновлень або створення нової копії цифрового вмісту або цифрової послуги для споживача[7, п.63].

10. Умова про те, що приведення у відповідність послуги для споживача буде безкоштовною. Споживач не повинен нести жодних витрат, пов’язаних із розробкою оновлення для цифрового вмісту чи

цифрової послуги [7, п.64]. Якщо усунути недолік не вдалось, наприклад, через невиправдані витрати продавця, споживач повинен мати право на зниження ціни або розірвання договору негайно, наприклад, якщо продавець раніше не зміг успішно привести цифровий контент або цифрову послугу у відповідність або коли від споживача не можна очікувати підтримувати впевненість у здатності продавця привести цифровий контент або цифрову послугу у відповідність через серйозний характер невідповідності [7, п.65].

11. Розрахунок зниження ціни, як через відсутність відповідності, так і через час, протягом якого споживач не міг отримувати цифровим контент чи послугу [7, п.66]

12. Період та умови про отримання даних, які споживач залишив про себе, під час отримання послуги, безкоштовно у машинозчитуваному форматі [7, п. 71].

13. Умови про попереднє погодження про оновлення і модернізацію контенту чи послуги, оскільки їх модифікація може істотно вплинути на інтерес споживача та його об'єктивну можливість користуватись послугою [7, п. 74].

14. Опис характеристик цифрових змін:

- ступінь модифікації, яка не буде впливати на первісне використання або доступ до цифрового контенту чи цифрової послуги.
- якість, функціональність, сумісність та інше основні функції, звичайні для цифрового вмісту або цифрових послуг того самого типу [7, п. 75].
- строк для завчасного попередження про модифікацію, для забезпечення права споживача зробити копію вмісту своїх даних, які оброблялись в процесі надання цифрової послуги [7, п. 76].
- умови про підтримку доступу до цифрового контенту чи цифрової послуги без додаткових витрат, без модифікації. У такому разі споживач не може розірвати договір безкоштовно

[7, п. 77]. Тому що факт модифікації не перешкоджає йому користуватись послугою.

У разі виникнення спору, споживач не має доводити технічні недоліки чи невідповідність отриманої послуги, оскільки, продавець володіючи знаннями та ноу-хау, технічної інформації та високотехнологічної допомоги перебуває у кращому становищі, ніж пересічний громадянин. Але продавець має доводити, що цифрова послуга відповідали вимогам у момент укладення договору та у весь час або протягом цього періоду [7, п. 59], за умови, що технічне середовище сподивача відповідало умовам отримання послуги і продавець повідомив про наслідки такої невідповідності. У такому разі відповідальність буде за споживачем.

Роль конкурентних ринків у цифровому секторі

Послуги цифрових платформ мають такі характеристики:

- економія масштабу — нульові витрати для залучення бізнесу та користувачів;
- сильні мережеві ефекти — здатність з'єднувати багато бізнес-користувачів із споживачами через багатогранність послуг, та їх взаємозалежність суб'єктів.
- ефекти блокування;
- вертикальна інтеграція в управлінні даними.

Усі ці характеристики в поєднанні з недобросовісною практикою підприємств, що надають основні послуги платформи, можуть призвести до суттєвого підриву конкурентоспроможності, вплинути на справедливість комерційних відносин між підприємствами [10, п.1].

Саме тому запровадження правил чесної конкуренції Регламентом ЄС № 2022/1925 від 14 вересня 2022 року, формує єдині правила і стандарти конкуренції на цифровому ринку.

Конкурентність знижується, через існування дуже високих бар'єрів для входу або виходу на ринок послуг цифрових платформ, включаючи високі інвестиційні витрати, які неможливо або нелегко

відшкодувати у разі виходу, а також відсутність або обмежений доступ до деяких ключових ресурсів цифрової економіки, наприклад, наборів даних [10, п.3].

Ринкові процеси часто неспроможні забезпечити справедливі економічні результати. Для усунення такої ситуації, деякі країни прийняли національні правила і обмеження, однак це посилить фрагментацію цифрового ринку, та відкине назад у вже пройдених етапах розбудови цифрової економіки.

Фрагментації можна уникнути, якщо буде застосовано набір узгоджених правових зобов'язань, щоб забезпечити конкурентоспроможні та справедливі цифрові ринки, що включають присутність захисників на внутрішньому ринку на користь економіки ЄС [10, п.8-9].

Нижченаведені суб'єкти цифрового ринку мають здатність впливати на велику кількість кінцевих користувачів і підприємств, що тягне за собою ризик недобросовісної ділової практики:

- X онлайн-посередницькі послуги,
- X онлайн-пошукові системи,
- X операційні системи,
- X онлайн-соціальні мережі,
- X послуги платформи обміну відео,
- X послуги міжособистісного зв'язку, незалежні від номера,
- X послуги хмарних обчислень,
- X віртуальні помічники,
- X веб-браузери
- X онлайн-рекламні послуги, включаючи рекламні посередницькі послуги [10, п.14].

Онлайн-платформи часто безпосередньо збирають особисті дані кінцевих користувачів з метою надання послуг онлайн-реклами, коли кінцеві користувачі використовують сторонні веб-сайти та програмні додатки, треті сторони також надають опосередковані дані онлайн-платформам про своїх користувачів, які використовували їх послуги.

Обробка з метою надання онлайн-рекламних послуг персональних даних третіх осіб надає конкурентні переваги. Подібні переваги є результатом:

- поєднання особистих даних кінцевого користувача, зібраних із основної онлайн-платформи, з даними, зібраними з інших веб-сайтів;
- перехресне використання персональних даних із основної онлайн-платформи в інших службах, які окремо надає платформа, зокрема послугах, які не надаються разом із відповідною основною послугою платформи або не підтримують її, і навпаки;
- вхід кінцевих користувачів до різних служб онлайн-платформ для об'єднання персональних даних [10, п.36]

Захист персональних даних в екосистемі цифрових платформ Інтернету Речей.

Масштаби збирання та спільного використання персональних даних суттєво зросли. Економічна та соціальна інтеграція, як результат функціонування внутрішнього ринку, спричинили істотне зростання транскордонних потоків персональних даних. Такі зміни вимагають наявності міцних та більш узгоджених засад щодо захисту даних.

Стрімкий технологічний розвиток і глобалізація призводять до виникнення нових труднощів для захисту персональних даних. Окремим викликом є формування довіри, що забезпечить розвиток цифрової економіки [4, п.п. 5,6,7].

Для вирішення проблем захисту персональних даних в ЄС, посилення захисту громадян держав-членів Союзу посилення механізмів захисту прав суб'єктів даних та принципів обробки даних було розроблено Загальний регламент захисту даних (далі — GDPR). Цей регламент встановлює більш прогресивні принципи охорони персональних даних, зокрема: законність, правомірність, прозорість,

цільове обмеження, мінімізація даних, точність, обмеження зберігання, цілісність, конфіденційність, підзвітність.

GDPR встановлює вищі стандарти стосовно інформованої згоди та обов'язків щодо повідомлення. Розширює перелік прав суб'єкта персональних даних, для зміцнення правової та практичної визначеності у способах контролю та управління даними, зокрема право бути поінформованим про збирання даних (ст.13-14), право доступу до даних (ст.15), право на виправлення (ст.16), право на стирання (право бути "забутим") (ст.17), обмеження опрацювання (ст. 18), право на мобільність (перенесення) даних (ст. 20), право на заперечення (ст.21), захист від профайлінгу (ст. 22) [4].

Гармонізація норм про надання цифрових послуг.

Глобальна мета прийняття Регламенту про цифрові послуги та цифровий контент це сприяння належному функціонуванню внутрішнього ринку із забезпеченням високого рівня захисту споживачів, шляхом встановлення загальних правил до умов контрактів між цифровими платформами та споживачами щодо постачання цифрового контенту чи цифрових послуг, зокрема, правила щодо:

- відповідності цифрового контенту або цифрової послуги договору,
- перелік засобів правового захисту у разі відсутності такої відповідності або ненадання постачання
- способи застосування цих засобів правового захисту,
- умови про модифікацію цифрового вмісту або цифрової послуги.

Якщо систематизувати виклад цих підходів, які описані у Преамбули DSA, отримаємо наступні вимоги до контрактів.

У Регламенті розрізняють посередницькі сервіси залежно від обсягів і технічних особливостей надання послуг. Зокрема:

простого каналу, яка складається з передачі в мережі зв'язку інформації, наданої одержувачем послуги, або надання доступу до мережі зв'язку;

кешування, яка складається з передачі в комунікаційній мережі інформації, наданої одержувачем послуги, що включає автоматичне, проміжне та тимчасове зберігання цієї інформації з єдиною метою підвищення ефективності подальшої передачі інформації до інших одержувачів за їх бажанням;

хостингу, яка складається із зберігання інформації, наданої одержувачем послуги та на його запит [17, с.69].

У DSA встановлюються моделі відповідальності для посередницьких сервісів, залежно від дій.

Наприклад, якщо надається послуга, яка полягає у зберіганні інформації, наданої одержувачем послуги, постачальник послуг не несе відповідальності за інформацію, що зберігається на запит одержувача послуги, за умови, що постачальник:

- не володіє фактичними знаннями про незаконну діяльність або незаконний контент і, що стосується позовів про відшкодування збитків, не знає про факти або обставини, з яких випливає незаконна діяльність або незаконний контент;
- отримавши такі знання чи обізнаність, оперативно вживає заходів для видалення або вимкнення доступу до незаконного контенту;

Тісно із DSA пов'язан регламент про цифрові ринки (DMA). Метою цього Регламенту є встановлення узгоджених правил, що забезпечують для всіх підприємств конкурентні та справедливі ринки в цифровому секторі в усьому Союзі, де присутні гейткіпери, на користь бізнес-користувачів і кінцевих користувачів.

Регламент застосовується до основних послуг платформи, які надаються або пропонуються гейткіперами для бізнес-користувачів, зареєстрованих у Союзі, або кінцевих користувачів, зареєстрованих або розташованих у Союзі, незалежно від місця заснування чи проживання

гейткіперів і незалежно від закону, який іншим чином застосовується до надання послуги.

Гейткіпер означає постачальника основних послуг платформи, що означає будь-яке з наступного:

(a) посередницькі послуги в Інтернеті;

(b) пошукові системи в Інтернеті;

(c) послуги соціальних мереж в Інтернеті;

(d) послуги платформи для обміну відео;

(e) незалежні від числа послуги міжособистісного зв'язку;

(f) операційні системи;

(g) послуги хмарних обчислень;

(h) рекламні послуги, включаючи будь-які рекламні мережі, рекламні біржі та будь-які інші послуги з рекламного посередництва, що надаються постачальником будь-якої з основних послуг платформи, перелічених у пунктах (a) – (g).

Постачальник послуг основної платформи *(a provider of core platform services)* визнається гейткіпером, якщо:

(a) він має значний вплив на внутрішній ринок;

(b) він керує основною платформою, яка служить важливим шлюзом для бізнес-користувачів, щоб до- сягти кінцевих користувачів;

(c) він займає міцне та довготривале положення в своїй діяльності або передбачається, що займе таку позицію в найближчому майбутньому [10].

Регулювання цифрової економіки в ЄС згідно з DMA, DSA та GDPR.

Важливо відзначити, що DMA, DSA та GDPR доповнюють загально-правову систему регулювання цифрової економіки в Союзі.

DSA не слід читати окремо: він застосовується на додаток до Загального регламенту захисту даних (GDPR) , разом із Законом про цифрові ринки (DMA), а також інших нормативних актів і директив законодавчого пакету Стратегії даних ЄС .

DSA встановлює низку юридичних зобов'язань:

- вимог щодо видалення вмісту,
- заборони брати участь у маніпулятивному дизайні
- заборони демонстрації реклами для профільованих користувачів на основі конфіденційних характеристик широкі зобов'язання підзвітності, що вимагають аудиту алгоритмів та оцінки системних ризиків.

Враховуючи структурну та системну значимість певних компаній в екосистемі цифрових послуг, DSA накладає суворіші зобов'язання на дуже великі онлайн-платформи (VLOP) і дуже великі онлайн-пошукові системи (VLOSE).

Такі компанії мають:

дотримуватися вищих стандартів прозорості,

надавати доступ до (особистих) даних компетентним органам і дослідникам,

виявляти, аналізувати, оцінювати та пом'якшувати системні ризики, пов'язані з їхніми послугами.

Такі системні ризики були класифіковані за чотирма різними категоріями [9, п.80-84]:

незаконний контент;

фундаментальні права (свобода вираження поглядів, плюралізм засобів масової інформації, права дітей, захист споживачів і недискримінація, серед іншого);

громадська безпека та виборчі/демократичні процеси;

охорона громадського здоров'я, з особливим акцентом на неповнолітніх, фізичне та психічне благополуччя.

Усі постачальники посередницьких послуг, включаючи онлайн-платформи, на які поширюється DSA, також є «контролерами» відповідно до GDPR у тій мірі, в якій вони обробляють персональні дані та приймають рішення щодо засобів і цілей такої обробки і саме тому вони мають дотримуватись вимог цих двох Регламентів.

10 сфер впливу DSA та GDPR на обробку даних.

1. Маніпулятивне проектування в онлайн-інтерфейсах;
2. Цільова реклама на основі конфіденційних даних;
3. Цільова реклама та захист неповнолітніх;
4. Системи рекомендацій без профілювання;
5. Системи рекомендацій і прозорість реклами;
6. Доступ до даних для дослідників і компетентних органів;
7. Видалення незаконного контенту;
8. Оцінка ризиків;
9. Комплаєнс-функція та законний представник DSA;
10. Відповідальність посередника та обов'язок надання інформації [18].

Маніпулятивне проектування в онлайн-інтерфейсах це практики, які суттєво спотворюють або погіршують, навмисно чи фактично, здатність одержувачів послуги приймати самостійні та усвідомлені вибори чи рішення; [9, п.67].

- практики, які забороняють постачальникам онлайн-платформ проектувати, організовувати або керувати своїми онлайн-інтерфейсами таким чином, щоб обманювати або маніпулювати одержувачами їхніх послуг або спосіб, який іншим чином істотно спотворює або погіршує здатність одержувачів їхніх послуг приймати вільні та обґрунтовані рішення [9, п.п. 25,67].

Цільова реклама на основі конфіденційних даних формує заборону постачальникам онлайн-платформ «представляти» рекламу користувачам, що випливає з їхнього профілювання [4, ст.26, 9, ст. 28].

Цільова реклама та захист неповнолітніх. Автоматизоване прийняття рішень, у тому числі профілювання не повинно застосовуватися до дітей і для будь-якого типу контексту, наприклад освітніх послуг [4, п.71], DSA посилює цей захист, коли йдеться про онлайн-платформи, забороняючи показ реклами на основі профілювання з використанням особистих даних користувачів, «якщо

вони з достатньою впевненістю знають, що одержувач послуги є неповнолітнім» Крім того, відповідно до принципу мінімізації даних [4, ст.5] ця заборона DSA не повинна спонукати постачальника онлайн-платформи «зберігати, отримувати або обробляти» більше особистих даних, ніж він уже має, для того, щоб оцінити, чи є одержувач послуги неповнолітнім [9, ст.28].

Системи рекомендацій і прозорість реклами. Означає, що «одержувачі послуги повинні мати доступ до інформації безпосередньо з онлайн-інтерфейсу, де представлена реклама, про основні параметри, які використовуються для визначення того, що конкретна реклама представлена для їх, надаючи змістовні пояснення логіки, яка використовується з цією метою» [9, п. 68].

Системи рекомендацій без профілювання. Такі вимоги є для VLOP і VLOSE «надавати принаймні один варіант для кожної зі своїх систем рекомендацій, який не ґрунтується на профілюванні» [9, п. 38].

Доступ до даних для дослідників і компетентних органів. Це включає доступ до даних, пов'язаних з алгоритмами, на підставі вмотивованого запиту та протягом розумного період а також координатора цифрових послуг «з єдиною метою проведення досліджень, які сприяють виявленню, ідентифікації та розумінню системних ризиків» у ЄС, а також «до оцінки адекватності, ефективності та впливу заходів із зменшення ризиків» [4, п. 34, 40]. Постачальники повинні анонімізувати або псевдонімізувати персональні дані, за винятком тих випадків, коли досягнення мети дослідження стає неможливим [4, п.98].

Основою DSA є зобов'язання служб хостингу, включно з онлайн-платформами, видаляти незаконний вміст:

стаття 16 DSA окреслює це зобов'язання на основі механізму сповіщення та вжиття заходів, які ініціюються після повідомлення будь-якої фізичної чи юридичної особи [9].

стаття 16, 17 GDPR надає особам право вимагати видалення своїх персональних даних за певних умов, а також право вимагати виправлення своїх даних [4].

Ці права «суб'єкта даних» відповідно до GDPR спрямовані на посилення контролю фізичних осіб над тим, як збираються, використовуються та поширюються їхні особисті дані. Стаття 3(h) DSA визначає «незаконний контент» як «будь-яку інформацію, яка сама по собі чи у зв'язку з діяльністю… не відповідає законодавству Союзу чи законодавству будь-якої держави-члена…, незалежно від конкретного предмета або природа цього закону». Як наслідок, оскільки «незаконний контент» за визначенням DSA також є особистими даними, особа потенційно може використовувати будь-який із способів, залежно від того, як на практиці пояснюється збіг цих двох положень. Примітно, що однією з підстав для отримання видалення персональних даних є «особисті дані, які були оброблені незаконно» і, отже, оброблені не відповідно до GDPR, що є законодавством Союзу.

Стаття 16 DSA підкреслює зобов'язання надавачів хостингових послуг, у тому числі онлайн-платформ, запровадити механізми для полегшення подання достатньо точних і адекватно обґрунтованих повідомлень. Стаття 12 GDPR, з іншого боку, вимагає від контролерів сприяти здійсненню прав суб'єкта даних, включаючи видалення, і повідомляти інформацію про вжиті дії без невиправданої затримки та в будь-якому випадку не пізніше ніж через місяць після отримання запиту.

Однак ключовою відмінністю є те, що в DSA запити на видалення вмісту також можуть надходити від органів влади (див. статтю 9 DSA) і від «довірених осіб, які позначають повідомлення» (стаття 22 DSA), з реалізацією цих прав може звернутись будь-яка фізична чи юридична особи. Навпаки, запити на видалення відповідно до GDPR можуть подавати лише суб'єкти даних (особи, чиї персональні дані обробляються), безпосередньо або через посередників, які діють від їх імені.

Оцінка ризиків. DSA, відповідно до статті 34, зобов'язує VLOP/VLOSE проводити оцінку ризиків принаймні раз на рік, щоб виявити, проаналізувати та оцінити «системні ризики, пов'язані з розробкою або функціонуванням їхніх послуг і пов'язаних із ними систем», включаючи алгоритмічні системи.

Є чотири системні ризики, які DSA просить включити в оцінку ризиків:

- поширення незаконного контенту;
- будь-які фактичні або передбачувані негативні наслідки для реалізації конкретних фундаментальних прав, серед яких згадуються право на повагу до приватного життя та право на захист персональних даних;
- будь-які фактичні або передбачувані негативні наслідки для громадянського дискурсу, виборчих процесів і громадської безпеки;
- будь-які фактичні передбачувані негативні наслідки, пов'язані з насильством за статтю, захистом громадського здоров'я та неповнолітніх, а також серйозні негативні наслідки для фізичного та психічного благополуччя особи.

Ті самі суб'єкти, швидше за все, зобов'язані проводити оцінку впливу на захист даних (DPIA). Серед елементів, які має містити DPIA відповідно до GDPR, є «оцінка ризиків для прав і свобод суб'єктів даних», які можуть виникнути через те, як контролери обробляють персональні дані за допомогою нових технологій, таких як алгоритмічні системи.

Функція "комплаєнс" та "юридичний представник" у нормах DSA. Відповідно до DSA, згідно зі статтею 41, призначені VLOP/VLOSE будуть зобов'язані створити «функцію відповідності», яка може складатися з кількох відповідальних осіб. Ця функція має бути:

- незалежною від їхніх операційних функцій;
- мати достатні повноваження, статус і ресурси;
- повинен мати доступ до керівного органу постачальника для моніторингу дотримання цим постачальником DSA.

Усі постачальники послуг, визначені як VLOP та VLOSE, які також є контролерами відповідно до GDPR, зобов'язані призначити спеціаліста із захисту даних (DPO).

Відповідальність посередника та зобов'язання надавати інформацію. GDPR і DSA перетинаються в сферах захисту даних, конфіденційності та відповідальності посередників. Це потенційно може включати обмін інформацією, в тому числі у випадках, коли вже зібрано особисті дані, з метою боротьби з незаконним вмістом в Інтернеті. У разі обміну та обробки даних постачальники посередницьких послуг повинні переконатися, що вони дотримуються заходів захисту GDPR.

Вищеописані сфери взаємодоповнення норм DSA та GDPR, вимагають послідовного тлумачення та застосування закону.

У структурі правозастосування та нагляду DSA не передбачає жодної офіційної ролі для співпраці чи координації, зокрема між DPA, Європейською радою із захисту даних або Європейським інспектором із захисту даних. Це не повинно бути перешкодою для налагодження процесів такої співпраці та координації в межах їхніх повноважень, оскільки розгортання DSA, ймовірно, розкриє складність взаємодії між двома законодавчими рамками навіть за межами десяти сфер, окреслених вище [18].

Список використаних джерел:

1. Дубняк, М. В., Грачова, О. Ю. (2023). Правове регулювання цифрової економіки. *Інформація і право*, (1 (44)), 79-87.
2. Баранов О.А. Трансформація: соціальна & цифрова & правова: монографія, у 3-х томах. Т. 1. Порятунок цивілізації: економіка результату. Одеса: Видавничий дім "Гельневтика", 2022, 272 с.
3. Дубняк М. (2023). Економіка даних: правовий та етичний аспект. *Інформація і право*, (3 (46)), 64-74.
4. 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) (Text with EEA relevance)
URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
5. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.)
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1807
6. Directive (EU) 2019/1024 of European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024
7. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770
8. Regulation (EU) 2020/0340 O European Parliament and of the Council of 25 November 2020 on European data governance (Data Governance Act)

URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767
9. 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)
URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022R2065
10. 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)
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925
11. 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
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925
12. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943
13. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj
14. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society

services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')
URL: https://eur-lex.europa.eu/eli/dir/2000/31/oj
15. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554
16. Дубняк, М. В. (2022). Захист комерційної таємниці суб'єктів індустрії інформаційних технологій в умовах євроінтеграції. *Нове українське право*, 1, 120-126.
17. Зайчук О., Король В., Нагнибіда В. (2022) Новітні підходи до регулювання інститутів цифрового права у законодавстві ЄС та перспективи для України. Вісник Національної академії правових наук України Том 29, № 2, С. 63-81
18. Zanfir-Fortuna G, Rovilos V (2023) EU's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR .
URL: https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/

Наукове видання

Олександр Андрійович БАРАНОВ
Ольга Михайлівна ГОЛОВКО
Марія Вікторівна ДУБНЯК

ГАРМОНІЗАЦІЯ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА ДО ЄВРОПЕЙСЬКИХ ПРАКТИК У СФЕРІ ІНТЕРНЕТУ РЕЧЕЙ

МОНОГРАФІЯ

В авторській редакції

Підписано до друку 01.11.2023.
Формат 60х84/16. Ум-друк. арк. 6,28.
Наклад 150 прим. Зам. № 2311-06.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net