With the support of the Erasmus+ Programme of the European Union

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»

ЗБІРНИК МАТЕРІАЛІВ
ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ІНТЕРНЕТ РЕЧЕЙ: ТЕОРЕТИКО-ПРАВОВІ ТА ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

29 квітня 2021 року, м. Київ

КИЇВ
2021

СКЛАД ОРГАНІЗАЦІЙНОГО КОМІТЕТУ:

Мельниченко А.А. - *кандидат філософських наук, доцент, проректор з навчальної роботи КПІ ім. Ігоря Сікорського.*

Цимбаленко Я.Ю. - *кандидат наук з державного управління, доцент, в.о. Декана Факультету соціології і права, КПІ ім. Ігоря Сікорського.*

Бевз С.І. - *доктор юридичних наук, доцент, в.о. завідувача кафедри господарського та адміністративного права, КПІ ім. Ігоря Сікорського.*

Баранов О.А. - *доктор юридичних наук, старший науковий співробітник, Керівник наукового центру цифрової трансформації і права Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України». Академічний лідер проекту «Європейська інтеграція: законодавство та Інтернет речей».*

Головко О.М. - *кандидат юридичних наук, старший викладач кафедри публічного права, КПІ ім. Ігоря Сікорського. Координатор проекту «Європейська інтеграція: законодавство та Інтернет речей».*

Дубняк М.В. - *кандидат юридичних наук, старший викладач кафедри інформаційного права та права інтелектуальної власності КПІ ім. Ігоря Сікорського. Менеджер проекту «Європейська інтеграція: законодавство та Інтернет речей».*

Видання рекомендоване до друку рішенням Вченої ради факультету соціології і права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
(протокол N 8 від 26.04.2021 року)

Інтернет речей: теоретико-правові та практичні аспекти впровадження в умовах Європейської інтеграції: матеріали Всеукраїнської науково-практичної конференції, (29.04.2021, м. Київ) : ел. збірник / Упоряд.: Баранов О.А., Головко О.М., Дубняк М.В. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 192 с.

У конференції взяли участь провідні експерти та вчені наукових установ і навчальних закладів, представники зацікавлених державних органів і громадських організацій.

Рекомендується науковцям, державним службовцям, підприємцям, юристам, 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.

Матеріали подано в авторській редакції.

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

Підтримка Європейською комісією випуску цієї публікації не означає схвалення змісту, який відображає лише думки авторів, і Комісія не може нести відповідальність за будь-яке використання інформації, що міститься в ній.

Зміст

Програмні питання конференції.....6

ПЛЕНАРНЕ ЗАСІДАННЯ.....7

Андрощук Геннадій
ШТУЧНИЙ ІНТЕЛЕКТ І ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ:
ПРОБЛЕМИ РЕГУЛЮВАННЯ.....7
Боднар Єлизавета
МОРАЛЬНО-ЕТИЧНІ ПРОБЛЕМИ ВИКОРИСТАННЯ.....15
РОБОТІВ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ: ПРАВОВИЙ КОНТЕКСТ.....15
Брайчевський Сергій
ПРОБЛЕМА ІДЕНТИФІКАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ІНТЕРНЕТУ
РЕЧЕЙ.....19
Волинчук Юлія, Ковальчук Надія, Бородавка Катерина
ІНТЕРНЕТ РЕЧЕЙ ТА WMS-СИСТЕМИ В ЛОГІСТИЧНІЙ
ДІЯЛЬНОСТІ ПІДПРИЄМСТВА.....23
Головко Ольга
СОЦІАЛЬНЕ ПІДПРИЄМНИЦТВО ТА ТЕХНОЛОГІЇ ІОТ:
ПРАВОВИЙ АСПЕКТ.....25
Доронін Іван
ПРАВОВІ ПРОБЛЕМИ ВИКОРИСТАННЯ DL-ТЕХНОЛОГІЙ ДЛЯ ДЕРЖАВНИХ
РЕЄСТРІВ.....28
Дубняк Марія
ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В GAME-DEV ІНДУСТРІЇ.....31
Закірова Світлана
ОНОВЛЕННЯ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ
ДАНИХ ЗА ПРИНЦИПАМИ ЄВРОПЕЙСЬКИХ СТАНДАРТІВ.....34
Колодій Інна
«ПРАВО НА ЗАБУТТЯ» ЯК СПОСІБ ЗАХИСТУ ПРАВА НА ПРИВАТНІСТЬ В МЕРЕЖІ
ІНТЕРНЕТ: РЕАЛІЇ ТА ПЕРСПЕКТИВИ.....38
Костенко Олексій
ІДЕНТИФІКАЦІЙНІ ДАНІ IoT: ПРОБЛЕМИ ФОРМУВАННЯ ЮРИДИЧНОЇ
ВІДПОВІДАЛЬНОСТІ ПРИ ЗАСТОСУВАННІ ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ.....42
Солончук Ірина
ЦИФРОВА ТРАНСФОРМАЦІЯ: ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ
(IoT) У СФЕРІ СУДОЧИНСТВА.....46

Студентські виступи.....51

Воронько Марина
ВІДКРИТІ ДАНІ ЯК СКЛАДОВИЙ ЕЛЕМЕНТ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ.....51
Полякова Ірина
ПРОБЛЕМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУДОЧИНСТВА І ДІЛОВОДСТВА В СУДАХ
УКРАЇНИ.....55
Sikorinska Alina
EUROPEAN UNION LEGISLATION ON CYBERSECURITY.....59

Царик Олександра
ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН ПРИ ЗДІЙСНЕННІ КРИПТОВАЛЮТНИХ ОПЕРАЦІЙ.....61
Ярош Ілля
ІНТЕРНЕТ РЕЧЕЙ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ.....66

Секції конференції.....71

Абрамович Ірина
ШТУЧНИЙ ІНТЕЛЕКТ У КРИМІНАЛЬНО-ПРАВОВОМУ РОЗРІЗІ.....71
Балінська Валерія
СТАН ВПРОВАДЖЕННЯ В МІСТАХ УКРАЇНИ ЕЛЕМЕНТІВ ТА МЕХАНІЗМІВ «РОЗУМНОГО МІСТА».....75
Березіна Катерина
ПОРІВНЯЛЬНО-ПРАВОВІ ДОСЛІДЖЕННЯ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА ТА ЗАКОНОДАВСТВА ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.....78
Belousova Katerina
LEGAL RESPONSIBILITY IN THE INFORMATION FIELD.....82
Butok Alexandra
CYBER-SECURITY IN TERMS OF TRANSLATION (BASED ON THE WEBSITES AND DOCUMENTS OF THE EUROPEAN UNION).....84
Bukhanets Viktoriia
PROSPECTS FOR THE IMPLEMENTATION OF STATE POLICY IN THE FIELD OF ARTIFICIAL INTELLIGENCE IN ACCORDANCE WITH EU POLICY.....87
Водько Юлія
ПОРІВНЯЛЬНО-ПРАВОВІ АСПЕКТИ ДОСЛІДЖЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ ТА ЗАКОНОДАВСТВА ДЕРЖАВ ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ.....90
Войтко А.
ПРАВОВІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У НАЦІОНАЛЬНОМУ ЗАКОНОДАВСТВІ ТА ЄВРОПЕЙСЬКОМУ ПРАВІ.....94
Геворкян Л. А.
ПРОБЛЕМИ ВИЗНАЧЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КОНТЕКСТІ ІНТЕРНЕТ РЕЧЕЙ.....98
Геращенко Яна
«ДЕРЖАВА У СМАРТФОНІ»: ШЛЯХ ДО ПОВНОЇ ЛЕГАЛІЗАЦІЇ ЕЛЕКТРОННИХ ПАСПОРТІВ ТА СУЧАСНИЙ СТАН ПИТАННЯ.....101
Голіченко Дмитро, Журбенко Данило
СУЧАСНІ ТЕНДЕНЦІЇ ПРАВОВОГО РЕГУЛЮВАННЯ КРИПТОВАЛЮТ В УКРАЇНІ ТА СВІТІ.....105
Гречко Ярослава
ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН ПРИ ВИКОРАСТАННІ ШТУЧНОГО ІНТЕЛЕКТУ.....109
Данілевич Д. Р.
ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ:.....112
ЙОГО ПРАВОСУБ'ЄКТНІСТЬ.....112
Добровольська А.Ю.
БЛОКЧЕЙН ІНІЦІАТИВИ ЄС: ЦИФРОВА ТА САМОСУВЕРЕННА ІДЕНТИЧНІСТЬ.....114

Іщенко А.А., Висоцький І.С.
ПОГЛЯД НА ПРАВОВІ ОСОБЛИВОСТІ І ПРОБЛЕМИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ МЕДИЦИНИ....116
Kisil Anastasiya
LEGAL REGULATION OF CRYPTOCURRENCY CIRCULATION IN UKRAINE....119
Корнійчук Наталія
ШТУЧНИЙ ІНТЕЛЕКТ ЯК ОБ'ЄКТ АВТОРСЬКОГО ПРАВА....121
Ланкін Сергій
ПРОБЛЕМИ ВИЗНАЧЕННЯ ПОНЯТТЯ ВІРТУАЛЬНИХ АКТИВІВ ТА СТАТУСУ КРИПТОВАЛЮТИ В УКРАЇНСЬКОМУ ЗАКОНОДАВСТВІ....124
Лаушкін Ілля
ПРАВОВІ АСПЕКТИ ТА ПРОБЛЕМИ НОРМАТИВНОГО РЕГУЛЮВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ....128
Луценко А. С.
ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВІЗАЦІЇ В АГРАРНІЙ ПРОМИСЛОВОСТІ....132
Diana Mazur
PROBLEM OF INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS DURING THE COVID-19 PANDEMIC....135
Мінькіна Дар`я
ПРАВОВЕ РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ З ПОЗИЦІЙ ЦИВІЛЬНОГО ЗАКОНОДАВСТВА....137
Ніжнік Владислав
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЗАКОНОДАВСТВІ УКРАЇНИ ТА КРАЇН ЄВРОПЕЙСЬКОГО СОЮЗУ....140
Ніколюк Аліна
ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ 144
Роженко Андрій
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УПРАВЛІННЯ ДЕРЖАВОЮ....147
Розгон Ольга
НЕОБХІДНІСТЬ УРЕГУЛЮВАННЯ КАТЕГОРІЙ АВТОНОМНІ РОБОТИ І ШТУЧНИЙ ІНТЕЛЕКТ У РОЗРІЗІ ДИСКУСІЇ КОНЦЕПЦІЇ ОНОВЛЕННЯ ЦК УКРАЇНИ....152
Строк Анастасія
ШТУЧНИЙ ІНТЕЛЕКТ В ЮРИСПРУДЕНЦІЇ: ПЕРСПЕКТИВИ ТА РИЗИКИ....155
Стужук Ольга
ВПРОВАДЖЕННЯ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У НАЦІОНАЛЬНОМУ ЗАКОНОДАВСТВІ....159
Ткаченко Анна
ПРАВОВЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ....161
Ткачук Тарас, Пономаренко Ірина
ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ ПРИВАТНОСТІ У МЕДИЧНІЙ СФЕРІ УКРАЇНИ ТА США 164
Пославський Денис, Сторчак Антон
ЗАВДАННЯ РОЗПОДІЛУ ВІДПОВІДАЛЬНОСТІ ПРИ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ....167
Томик Вікторія
ПРАВОВЕ РЕГУЛЮВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В УКРАЇНІ....170

Тімашов Віктор, Ніколаєва Людмила, Дем’яненко Едуард
ПРОБЛЕМИ ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ В СФЕРІ ОХОРОНИ ЗДОРОВ‘Я.....174
Чесницький Данило
ПРАВОВИЙ СТАТУС НЕВЗАЄМОЗАМІННИХ ТОКЕНІВ (NFT).....176
Чорнобай Евеліна
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В ДЕРЖАВНОМУ СЕКТОРІ УКРАЇНИ.....180
Шершньова Анастасія
ПРАВОВЕ РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН У СФЕРІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ. ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД.....184
Щепеткова Вікторія
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ.....187
Післямова.....191

Програмні питання конференції

Секція 1. Проблеми правового регулювання суспільних відносин в сфері застосування штучного інтелекту, робототехніки, криптовалют, технологій блокчейн «хмарних» технологій, «великих даних» та інших складових Інтернету речей.

Секція 2. Правове забезпечення цифрової трансформації на основі впровадження технологій Інтернету речей у різних сферах діяльності: економіці, Індустрії 4.0, сільському господарстві, охороні здоров’я, комунальному господарстві (розумні міста, вулиці, будинки), транспорті (автономні автомобілі, розумні дороги, дрони тощо), управлінні державою, роздрібної торгівлі тощо.

Секція 3. Порівняльно-правові дослідження національного законодавства та законодавства Європейського Союзу з питань забезпечення кібербезпеки та вільного обігу даних, захисту персональних даних, застосування хмарних технологій та технологій блокчейну тощо.

Секція 4. Проблеми визначення юридичної відповідальності при застосуванні технологій Інтернету речей.

ПЛЕНАРНЕ ЗАСІДАННЯ

Андрощук Геннадій

кандидат економічних наук, доцент,
головний науковий співробітник НДІ
інтелектуальної власності НАПрН України

ШТУЧНИЙ ІНТЕЛЕКТ І ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ: ПРОБЛЕМИ РЕГУЛЮВАННЯ

Генеральний директор Всесвітньої організації інтелектуальної власності (ВОІВ) Дарен Танг в ключовій доповіді ВОІВ «Світові показники діяльності в галузі інтелектуальної власності» (World Intellectual Property Indicators 2020) зазначає «Активне використання інструментів інтелектуальної власності свідчить про високий рівень інновацій і творчості в кінці 2019 р. якраз на початку пандемії COVID-19. Пандемія зміцнила тенденції, що давно зароджувалися, шляхом стимулювання використання нових технологій і прискорення цифровізації у повсякденному житті. Оскільки інтелектуальна власність настільки тісно пов'язана з технологіями, інноваціями і процесом цифровізації в світі, після закінчення пандемії вона стане ще важливішою для більшої кількості країн» [1]. Згідно визначення за стандартом ISO/IECTR 24028:2020 [2], штучний інтелект (ШІ) – це здатність сконструйованих систем набувати, обробляти та застосовувати знання та навички. Водночас Європейська Комісія визначає ШІ як системи, які демонструють розумну поведінку завдяки аналізу їхнього оточуючого середовища та вжиття дій – з певним рівнем автономності – для досягнення визначених цілей [3]. Штучний інтелект (ШІ) в правовому регулюванні розглядається як новий виклик для економіки та правової системи, нове явище, що має мультиплікаційний ефект, правовий феномен в структурі правовідносин, новий об'єкт для правового регулювання. Сучасний науково-технологічний розвиток привів до того, що ШІ став здатний генерувати та створювати різні твори – науки, літератури і мистецтва. Створення творів ШІ є невід'ємною сферою діяльності в сучасній цифровій економіці. Ці обставини висувають на передній план проблеми визнання авторства при створенні творів ШІ, можливості розпорядження авторами своїми правами і використання ними механізмів правової охорони об’єктів інтелектуальної власності (ІВ). Результатом правового регулювання в Україні питань, пов'язаних з наявністю або відсутністю правосуб'єктності у ШІ, буде формування чіткого розуміння права в

сфері використання результатів діяльності ШІ. У зв'язку з тим, що в національному законодавстві у сфері ІВ питання щодо самостійної правосуб'єктності ШІ не вирішене, доцільно звернутися до аналізу зарубіжного законодавства та доктринальних позицій з цієї проблеми.

Згідно зі звітом Відомства інтелектуальної власності Великобританії (IPO) «Штучний інтелект: всесвітній огляд патентів на AI і патентування в секторі AI Великобританії» (Artificial Intelligence: A worldwide overview of AI patents and patenting by the UK AI sector), кількість опублікованих патентних заявок, що стосуються ШІ, за останнє десятиліття збільшилася на 400%. Кількість патентних заявок з використанням технології ШІ, поданих в США, збільшилася вдвічі в період з 2002 до 2018 року. ВОІВ розпочала серію консультацій про ШІ і інтелектуальну власність. Постійно обговорюється питання про те, чи слід захищати творіння ШІ авторськими правами, правами на дизайн, патентами або правами особливого роду - sui generis, або не захищати їх взагалі.

Можна застосовувати підхід, що все, створюване ШІ або з його використанням, належить власникові ШІ, як це передбачено ч. 2 ст. 189 Цивільного кодексу України «Продукція, плоди та доходи». Однак ця норма уточнює «якщо інше не встановлено договором або законом». Водночас науковцями нині пропонуються різні підходи, починаючи від суб’єктивних (хто може бути творцем і носієм вольового компоненту, що ініціює створення об’єкту ІВ, концепція «Sweat of the brow») до суто правових (визнання інформацією з відкритим доступом, суспільним надбанням; ліцензії Creative Commons, критерії охороноздатності, обмеження монопольних прав суб’єкта права ІВ у просторі та часі).

Нині в багатьох країнах авторські права надаються тільки на твори інтелектуальної творчості людини. Бюро реєстрації авторських прав США заявляє: «Бюро охорони авторських прав США зареєструє оригінальний авторський твір за умови, що твір створений людиною». У п. 3 ст. 9 Закону Великобританії «Про авторське право, дизайн і патенти» зазначається, що «стосовно літературного, драматичного, музичного або художнього твору, згенерованого комп'ютерною системою, автором буде вважатися особа, за допомогою якої вживаються заходи, необхідні для створення твору». Так само Австралійське і Європейське патентне відомство (ЄПВ) у багатьох випадках визнавали і надавали патентні права тільки на об’єкти, створені людиною. Деякі країни вважають за краще визнати зусилля, прикладені для створення ШІ, який надає творчий контент. До таких країн належать Індія, Великобританія, Ірландія, Нова Зеландія і Гонконг. Отже, програміст ШІ отримує авторство творів.

Європейське патентне відомство (ЄПВ) опублікувало своє рішення від 27 січня 2020 р. із викладенням причин відмови в двох європейських патентних заявках, в яких система ШІ була позначена як винахідник. Подані фізичною особою восени 2018 р., заявки EP 18 275 163 і EP 18 275 174 були відхилені ЄПВ після усного розгляду з заявником в листопаді 2019 р. на тій підставі, що вони не відповідають юридичним вимогам Європейської патентної конвенції. (EPC), що винахідник, вказаний у заявці, має бути людиною, а не машиною. ВПТЗ США, Європейське патентне відомство (ЄПВ) і Відомство інтелектуальної власності Великобританії (UKIPO) відмовили в дозволі називати ШІ винахідником в патентних заявках. У січні 2020 р. ЄПВ і UKIPO відхилили заявки на патенти, в яких DABUS був позначений як винахідник. UKIPO опублікувало рішення, в якому зазначалося, що заявка має бути відкликана, оскільки DABUS не є особою, передбаченою Законом про патенти, і не може вважатися винахідником. У висновку ЄПВ пояснило, що назва машини не відповідає вимогам правила 19 (1) EPC, яке вимагає прізвища, імені та повної адреси винахідника. ЄПВ також пояснило, що потрібно законодавство для створення юридичної особи для систем або машин ШІ, тому що «історія законодавства показує, що законодавці EPC були згодні з тим, що термін «винахідник» відноситься тільки до фізичної особи». ЄПВ також вказало, що вимога, щоб винахідник був фізичною особою є «міжнародно застосовним стандартом», якому слідує більшість країн-учасниць EPC, а також Китаю, Японії, Кореї і США. Крім того, ЄПВ заявило, що «не визначено національного закону, який [визнавав би] річ, зокрема систему Al або машину, як винахідника» [4].

Наведемо перший судовий прецедент у сфері авторського права. У січні 2020 р. суд у Шеньчжені, провінція Гуандун (КНР), постановив, що твір, створений ШІ, може бути захищений авторським правом. Рішення було прийнято після того, як технічний гігант Tencent подав до суду на онлайн-платформу, яка надає інформацію про кредити за копіювання статті, написаної роботом Tencent Dreamwriter, без дозволу. Dreamwriter - це автоматизована програма для написання новин, заснована на даних і алгоритмах, розроблена Tencent у 2015 році. Dreamwriter 20 серпня 2018 р. написав фінансовий звіт, що включає індекс Шанхая за цей день, обмін валюти і рух капіталу. У статті, опублікованій на веб-сайті Tencent Securities, зазначено, що «стаття була автоматично написана Tencent Robot Dreamwriter». Пізніше компанія Shanghai Yingxun Technology скопіювала її на свій сайт. Народний суд району Наньшань заявив, що відповідач - Shanghai Yingxun Technology Company - порушив авторські права Tencent і повинен нести цивільну відповідальність. Суд заявив, що форма вираження статті відповідає вимогам письмового твору, а зміст показав вибір, аналіз і оцінку відповідної інформації і даних про фондовий ринок. Це свідчить, що

структура статті була розумною, логіка - зрозумілою, і у ній була відповідна оригінальність. З огляду на те, що відповідач вилучив роботу, що порушує авторські права, шанхайській компанії Yingxun Technology було наказано виплатити Tencent 1500 юанів (216 дол. США) за економічні втрати і порушення прав.

А ось приклад з української практики. Гурт "Океан Ельзи" ("ОЕ") 12 лютого ц.р. випустив нову пісню і кліп до неї. Фронтмен гурту Святослав Вакарчук 16 лютого у своєму Twitter написав, що автором пісні є штучний інтелект. Цю програму розробив аспірант університету Джонстона - Кйеф Ріш. За його словами, програма послухала все пісні "ОЕ" і написала свою. Композиція вийшла в звичному для цієї групи стилі, і якщо б С. Вакарчук не розкрив секрет, то ніхто б і не сумнівався щодо авторства [5].

На підставі аналізу розглянутих судами справ, пов'язаних з проблемою правосуб'єктності ШІ, і вивчення законотворчої діяльності з цього питання, дослідниками вказується, що для вирішення проблеми визначення прав ІВ на створений ним твір, можливі такі варіанти: 1. Не наділяти ШІ правами автора і не визнавати створений твір об'єктом ІВ. 2. Визнати за ШІ права автора. 3. Розподілити авторські права між ШІ і фізичною особою, яка брала участь у діяльності ШІ. 4. Наділити авторськими (патентними) правами фізичну особу, яка створювала ШІ або набувала його для створення творів (винаходів). 5. Створити неіснуючого автора і наділити його правами на створений твір [6,с.182]. При цьому автор цієї статті дотримується точки зору щодо передачі таких прав власнику або творцеві ШІ (в залежності від обставин).

Представляє інтерес Резолюція Європейського парламенту від 20 жовтня 2020 р. про права інтелектуальної власності в області розробки технологій штучного інтелекту (2020/2015 (INI)) [7]. Викладемо основні положення цього документу. Європейський парламент взяв до відома Білу книгу Європейської комісії з штучного інтелекту - європейський підхід до досконалості і довіри і європейську стратегію обробки даних; підкреслив, що викладені тут підходи можуть допомогти розкрити потенціал ШІ, орієнтованого на людину, в ЄС; проте **зазначив, що захист прав інтелектуальної власності (ІВ) в контексті розвитку ШІ і пов'язаних з ним технологій не було взято до уваги Комісією, незважаючи на ключове значення цих прав**; Підкреслює важливість створення діючої і повністю узгодженої нормативно-правової бази для технології ШІ; Підкреслює, що для розкриття потенціалу технологій ШІ необхідно усунути непотрібні юридичні бар'єри, щоб не перешкоджати зростанню та інновацій в економіці ЄС, що розвивається; закликає до оцінки впливу на захист прав ІВ в контексті розвитку технологій ШІ; Вважає, що Союз може відіграти провідну роль у розвитку технологій ШІ, якщо він прийме

добре функціонуючу нормативно-правову базу, яка буде регулярно оцінюватись у світлі технологічних досягнень, і буде проводити активну державну політику; особливо щодо програм навчання і фінансової підтримки досліджень, а також співпраці між державним і приватним секторами; підкреслює роль системи патентного захисту в заохоченні створення винаходів ШІ і сприяння їх поширенню; і необхідність створення можливостей для європейського бізнесу та стартапів для підтримки розробки та впровадження ШІ в Європі; Зазначає, що стандартизовані патенти відіграють ключову роль в розробці та поширенні нового ШІ і пов'язаних з ним технологій, а також в забезпеченні функціональної сумісності; закликає Комісію підтримати встановлення галузевих стандартів і заохочувати формальну стандартизацію; Вказує, що патентна охорона може бути надана до тих пір, поки винахід є новим, неочевидним і є результатом інноваційної діяльності; далі зазначає, що патентне право вимагає всебічного опису базової технології, що може бути проблематичним для деяких технологій ШІ через складність аргументів;підкреслює правові проблеми зворотного проектування, яке є винятком з захисту авторських прав на комп'ютерні програми та захисту комерційної таємниці, які, в свою чергу, необхідні для інновацій і досліджень і які слід належним чином враховувати в контексті розвитку технологій ШІ; Закликає Комісію оцінити можливість адекватного тестування продуктів, наприклад, в модульному режимі, без ризику для власників прав ІВ або щодо комерційної таємниці в результаті розкриття великої кількості інформації, що легко відтворюється, про продукти; підкреслює, що технології ШІ повинні бути вільно доступні для освітніх і дослідницьких цілей, наприклад для більш ефективних методів навчання; рекомендує, щоб всі права власності надавалися тільки фізичним або юридичним особам, законно створив твір, і тільки за згодою правовласника, підкреслює важливість полегшення доступу до даних і обміну даними, відкритих стандартів і технологій з відкритим вихідним кодом при одночасному заохоченні інвестицій і стимулюванні інновацій; якщо використовується матеріал, захищений авторським правом, якщо не застосовуються виключення або обмеження авторського права; підкреслює важливість полегшення доступу до даних і обміну даними, відкритих стандартів і технологій з відкритим вихідним кодом при одночасному заохоченні інвестицій і стимулювання інновацій; зазначає, що ШІ або пов'язані з ним технології, використовувані в процесі реєстрації ПІВ і відповідальності, не можуть замінити індивідуальну перевірку, проведену людьми, для забезпечення якості та справедливості рішень; Підкреслює важливість повної реалізації Стратегії єдиного цифрового ринку для поліпшення доступності та взаємодії неособистих даних в ЄС; підкреслює, що європейська стратегія обробки даних повинна забезпечувати баланс між просуванням потоку даних, широким

доступом, використанням та спільним використанням та захистом прав ІВ та комерційної таємниці при дотриманні принципів захисту даних і конфіденційності;

Ще одним важливим документом , що заслуговує на увагу, є **Резолюція Міжнародної асоціації з охорони інтелектуальної власності (AIPPI) 2020 р.,** яка налічує близько 9000 членів по всьому світу з більш ніж 125 країн. Питання для вивчення – Патенти. Інвентаризація винаходів, створених із використанням штучного інтелекту (Resolution 2020 – Study Question – Patents Inventorship of inventions made using Artificial Intelligence), затверджена на щорічному всесвітньому конгресі AIPPI World Intellectual Property Congress 2020, що відбувся в режимі онлайн в жовтні 2020 р. Розглянемо її основні положення [8]. Незалежно від того, чи був використаний ШІ при розробці винаходу, фізичну особу слід вважати винахідником або співавтором, якщо вона внесла інтелектуальний внесок у винахідницьку концепцію. Якщо фізична особа розробила алгоритм ШІ для вирішення наперед визначеної проблеми, яка ефективно вирішується винаходом, така фізична особа повинна розглядатися як винахідник винаходу. Якщо алгоритм ШІ являв собою загальний алгоритм ШІ, розроблений без урахування конкретної проблеми, фізичну особу, яка розробила алгоритм ШІ, не слід вважати винахідником, якщо він не має іншого інтелектуального внеску в концепцію винаходу. с. Фізичну особу, яка вибирає дані або джерело даних для навчання алгоритму ШІ, слід вважати винахідником або співавтором винаходу, створеного за допомогою цього алгоритму ШІ. Фізичну особу, яка вибирає або генерує дані, або обирає джерело даних для введення в навчений алгоритм ШІ, слід вважати винахідником або співавтором винаходу, створеного за допомогою цього алгоритму ШІ, якщо дані або джерело даних генеруються або обрані з метою вирішення наперед визначеної проблеми і винахід ефективно вирішує проблему. Фізичну особу, яка визнає, що результат алгоритму ШІ є винаходом, слід вважати винахідником або співавтором такого винаходу. ШІ не слід вважати винахідником або співавтором винаходу, а також забороняється називати його таким, якщо жоден внесок у винахід фізичної особи не ідентифікується. З метою сприяння інноваціям винаходи, створені з використанням ШІ, не повинні виключатись із патентної охорони як такі, незалежно від того, чи є достатня кількість внесків фізичної особи, яка може бути названа винахідником, і за умови, що існує фізична або юридична особа, зазначена заявником.

Висновки. Штучний інтелект - одна з найважливіших технологій подвійного призначення, що має мультиплікаційний ефект, перетворює економіку і суспільство і сприяє глобальній цифровій трансформації. ШІ використовується у всіх сферах, включаючи транспорт, телекомунікації, біологічні науки і медицину, персональні

пристрої і безпеку. ШІ є багатоцільовою технологію, яка знаходить широке застосування в економічній та соціальній сферах. Він значно впливає на процеси створення, виробництва та розподілу товарів і послуг економічного і культурного призначення, а в майбутньому цей вплив ще більше посилиться. Можна говорити про наявність різних точок дотику ШІ, з одного боку, і політики в області ІВ, з іншого, оскільки однією з основних цілей політики в області ІВ є стимулювання інновацій і творчості в рамках економічних і культурних систем. Системи ІВ покликані мотивувати людей на винахідницьку діяльність і творчість. Саме здатність до інноваційної і творчої діяльності до недавнього часу була визначальною характеристикою людини. Послідовний розвиток ШІ як універсальної технології, що знайшла широке застосування в економіці, ставить ряд принципових питань, які зачіпають основи існуючих систем ІВ. Для багатьох держав світу ШІ перетворився в один з компонентів їх стратегічного потенціалу. Держави все частіше впроваджують стратегії розвитку ШІ-потенціалу, а також вживають заходів щодо його регламентації. ШІ ставить ряд складних питань, які потребують глобального вирішення. У зв'язку з цим ВОІВ почала займатися аспектами ШІ, специфічними для ІВ. За ініціативи ВОІВ проводиться Дискусія з питань ІВ та ШІ, у рамках якої держави-члени на міжнародному рівні обговорюють вплив ШІ на ІВ, з метою спільно визначити коло питань, що потребують уваги законодавців, а також допоможуть сформувати урядові та міжнародні політики використання ШІ у сфері ІВ. Україна, як держава-член організації та учасниця багатьох міжнародних договорів у сфері ІВ, бере активну участь в обговореннях та багатосторонніх форумах. Одним із векторів взаємодії ВОІВ та Державної системи правової охорони інтелектуальної власності на 2021 рік визначено роботу з імплементації інструментарію та досвіду використання технології ШІ в роботі патентних відомств та індустрії загалом. Викладений аналіз законодавчої та правозастосовної практики, регіональних та міжнародних документів щодо регулювання питань ШІ і ІВ покликаний сформувати єдиний уніфікований підхід до тлумачення критеріїв охороноздатності результатів діяльності ШІ в різних юрисдикціях, використання механізмів правової охорони об’єктів ІВ, підкреслити важливість політики в сфері ІВ для національної безпеки.

Література:

1.World Intellectual Property Indicators 2020. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2020.pdf (дата звернення: 14.02.2021).

2.ISO/IEC TR 24028:2020: Information technology — AI — Overview of trustworthiness in AI. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24028:ed-1:v1:en (дата звернення 05.04.21)

3.Independent High-Level Expert Group On Artificial Intelligence Set Up By The European Commission. A Definition Of AI: Main Capabilities And Disciplines. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341 (дата звернення 05.04.21)

4. The Year in Patents: Ten Developments We'll Remember From 2020. URL:https://www.ipwatchdog.com/2020/12/31/year-patents-ten-developments-well-remember-2020/ id=128674/ (дата звернення 05.04.2021).

5. Клочко О. Штучний інтелект написав замість Вакарчука нову пісню для "Океану Ельзи". URL: https://life.comments.ua/ua/news/music/shtuchniy-intelekt-napisav-zamist-vakarchuka-novu-pisnyu-dlya-okeanu-elzi-video-671941.html (дата звернення 05.04.2021).

6. Морхат П.М., Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дисс. … д-ра юрид. наук. РГАИС. Москва. 2018. С. 243.

7. Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji. URL: (2020/2015(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PL.html (дата звернення 05.04.2021).

8. Artificial Intelligence. URL: https://aippi.soutron.net/Portal/DownloadImageFile.ashx?objectId=8497 (дата звернення 05.04.2021).

Боднар Єлизавета

студентка магістратури юридичного факультету ДВНЗ «Ужгородський національний університет»
Науковий керівник: Головко О.М.,
к.ю.н., старший викладач
кафедри публічного права
КПІ ім. Ігоря Сікорського

МОРАЛЬНО-ЕТИЧНІ ПРОБЛЕМИ ВИКОРИСТАННЯ РОБОТІВ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ: ПРАВОВИЙ КОНТЕКСТ

Належний морально-етичний розвиток досягається як глобальна стратегія вирішення головної суспільної суперечності між зростаючими потребами людства і неможливістю задоволення усіх людських потреб. Зазначену суперечність можливо вирішити лише в процесі пошуку аксіологічної раціональності суспільного функціонування, що може бути тільки завдяки «прищепленню» певних цінностей і моральних норм.

В Україні нині обговорюється Концепція розвитку сфери штучного інтелекту в Україні. Однак згаданий документ не містить правових рекомендацій щодо розвитку використання штучного інтелекту, в ньому лише сказано, що розробники мають дотримуватися права на конфіденційність і прайвесі людини (планується розробити Етичний кодекс використання штучного інтелекту, враховуючи європейський досвід). Тому актуальним є створення правової Карти використання штучного інтелекту – аналітичного, полісі-документу, який має містити бачення громадянського сектору щодо пріоритетів використання та розвитку правового середовища для розробників та користувачів штучного інтелекту. Одним із перших реальних кроків на шляху до законодавчого закріплення стандартів розробки та використання штучного інтелекту є прийнята Резолюція ЄС від 16 лютого 2017 року із рекомендаціями Комісії щодо правил цивільно-правового регулювання робототехніки. Хартія робототехніки, яка додається до резолюції, була розроблена науковим підрозділом з оцінки розвитку науки і технологій та дослідницьким центром Європарламенту. Хартія містить кодекс етичних норм для розробників у сфері робототехніки, кодекс комітетів по етиці наукових досліджень, а також ліцензії для розробників і користувачів.

У сучасній доктрині права до основних положень можна віднести те, що система правових норма призначена для регулювання найбільш значущих

суспільних відносин між суб'єктами, в якості яких можуть виступати юридичні та фізичні особи в найширшому їх тлумаченні. Крім того, в сучасній доктрині права стверджується, що система правових норм регулює найбільш важливі, принципові відносини, що мають істотне значення для інтересів держави, суспільства, нормальної життєдіяльності людей. Це означає, що норми права призначені для регулювання життєве важливих суспільних відносин, відсутність регулювання яких значно знижує ефективність соціальної взаємодії між членами суспільства. При цьому правознавці вважають: всі види і форми відносин, що виникають і відбуваються в суспільстві між індивідами та їх об'єднаннями з приводу об'єкта цих відносин, який може мати як матеріальний, так і нематеріальний зміст, є (на відміну від взаємозв'язків у природі) суспільними або соціальними відносинами.

Важливо відзначити, що мораль і право, як головні соціальні регулятори, що поєднані між собою та доповнюють один одного, є наслідком творчої діяльності інтелекту особи (навіть у тому разі, коли вважається, що до розроблення цих настанов певну особу надихнула інша вища сила, що притаманно практично для всіх релігій; або незбагненні коливання інформаційного простору [1, с. 98].

Особа пізнає норми моралі протягом всього власного життя, причому наслідок основного навчання слід маніфестувати тільки на чітко обумовлених етапах соціальної відповідності (подолання випробувань у певних обрядах переходу від стану дитини до стану чоловіка-воїна, присяга військового, ініціація під час обряду шлюбу, яка визначає вмирання старого та народження нового статусу певної людини тощо), або він презюмується, виходячи з вимог закону (наприклад, фактором встановлення 14- або 16-річного віку кримінальної відповідальності вважається переконання у тому, що людина, яка виховувалася у суспільстві, тобто серед людей, має на час досягнення вказаного віку засвоїти основні норми співжиття суспільстві). Важливо відзначити, що для штучного інтелекту не є складним вивчити, проаналізувати та систематизувати певні моральні та правові норми у більш короткий етап часу, ніж це вимагається від особи. Тож питання про те, чи може штучний інтелект засвоїти норми моралі, або чи зможе він спиратися на ці норми у власній поведінці ймовірніше має позитивну відповідь [2, с.12].

Цілком очевидно, що для кожного конкретного виду людської діяльності вченими і практиками, в тому числі, і дослідниками в галузі права, може бути складений повний і точний перелік когнітивних функцій, необхідних для її реалізації. Власне, цей перелік і буде своєрідними технічними вимогами для створення ШІ, орієнтованого на використання в конкретному виді діяльності. Для цілей правового аналізу змісту суспільних відносин не важливо знання технічних або технологічних особливостей технічних засобів, за допомогою яких вони

реалізуються. Це відповідає одному з фундаментальних принципів правової доктрини – технологічної нейтральності правового регулювання [3, с. 18].

Технічні або технологічні особливості деяких засобів, в тому числі і штучного інтелекту, які використовуються під час реалізації суспільних відносин, можуть викликати тільки деякі особливості реалізації цих відносин, що в свою чергу зумовлює можливість появи деяких особливостей правового регулювання, яке в основі своїй залишається незмінним. Іноді, вчені та практики юристи висловлюють думку про те, що використання нових технологій при реалізації суспільних відносин призводить до необхідності створення нового законодавства або навіть нових галузей права. Але виникає майже природне бажання виокремити правові норми, що регулюють зазначені «нові» типи суспільних відносин, для більш зручнішого їх вивчення та теоретичного узагальнення. І в цьому бажанні виокремлення лунають пропозиції про створення нових галузей права [4, с. 276].

Оскільки традиційна система права, що існувала на той момент, не мала пропозицій з регулювання суспільних відносин, які реалізуються за допомогою нових технологій, то це привело до формування невеликої кількості нових правових норм регулювання суспільних відносин. Ці нові правові норми згодом природним чином стають гармонійною частиною традиційної системи правового регулювання безлічі однорідних суспільних відносин, об'єднаних загальною функціональною спрямованістю і загальним типом об'єктів в рамках якого і з'явився цей «новий» тип відносин.

Отже, штучний інтелект в інтересах правової науки, як і дефініції багатьох інших нових явищ (засобів, виробів, предметів тощо), які і сьогодні, і в майбутньому будуть або об'єктом суспільних відносин, або тим, за допомогою або на основі чого будуть реалізовуватися суспільні відносини, повинна відображати тільки специфіку реалізації суспільних відносин, яка власне і буде обумовлена використанням штучного інтелекту із зазначенням мінімально необхідних технічних подробиць [5, с.6].

Практично всі великі корпорації технологічного напрямку в усіх країнах активно розробляють або вже впроваджують «роботів», призначених для використання в самих різних видах людської діяльності, пов'язаної як з фізичними діями, так і з інтелектуальними або, іншими словами, пов'язаної із здійсненням певних дій як з матеріальним, так і з нематеріальним змістом об'єктів [6, с. 165]. Таке сприйняття поняття «робот» має дуже важливе значення для проблематики інтернету речей, так як саме роботи дозволяють виконувати різні послуги та проводити роботи завдяки наявності різноманітних виконавчих пристроїв. Цілком очевидно, що в умовах застосування технологій IP роботизація стає необхідною для

об'єктивізації в реальному світі результатів реалізації штучним інтелектом деяких когнітивних функцій [7, с.5].

Отже, для того, щоб використання штучного інтелекту людьми було максимально ефективним та безпечним, необхідно встановити чіткі правові засади для цього. Але, до сьогоднішнього дня, серед широкого кола фахівців і вчених, в тому числі юристів, все ще превалює футурологічне сприйняття роботів зі штучним інтелектом, в той час як найбільш розвинені країни світу вже використовують AI для подолання проблем не тільки локального, але й глобального характеру. В той же час, використання AI потребує врегулювання багатьох морально-етичних питань, що може бути здійснено шляхом передбачення правових механізмів вирішення найбільш ймовірних правових спорів у цьому напрямі.

Література:

1. Теоретичні та прикладні питання державотворення : електрон. наук. фах. вид. / Одес. регіон. ін-т держ. упр. Нац. акад. держ. упр. при Президентові України. Одеса : ОРІДУ НАДУ, 2019. Вип. 24. 112 с.
2. Симончук О. «Як роботизація змінює журналістику». URL: /http://ua.telekritika.ua/society/yak-robotizats%D1%96ya-zm%D1%96nyu%D1%94-zhurnal%D1%96stiku-675682(дата звернення: 13.04.2021)
3. Ілюхин О. «Людям улучшили память, вшив в мозг специальный чип». URL: https://hitech.vesti.ru/article/690129/(дата звернення: 12.04.2021)
4. Рассел С., Норвиг П. Искусственный интеллект: современный подход Artificial Intelligence: A Modern Approach (AIMA). 2-е изд. Москва: «Вильямс», 2007. 1424 с.
5. Чапек К. «Россумські Універсальні Роботи». URL: http://www.lib.ru/SOCFANT/CHAPEK/rur.txt(дата звернення: 12.04.2021)
6. Шелли М. Франкенштейн, или Современный Прометей. Последний человек. Москва: «Наука», «Ладомир», 2010. 667 с.
7. Марценко Н. Правовий режим штучного інтелекту в цивільному праві. URL: file:///C:/Documents%20and% 20Settings/Admin/%D0%9C% D0%BE %D0%B8%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD %D1%82%D1%8B/Downloads/884-1739-1-SM.pdf (дата звернення: 15.04.2021)

Брайчевський Сергій
кандидат фізико-математичних наук,
старший науковий співробітник
ДНУ «Інститут інформації, безпеки і права
Національної академії правових наук України»

ПРОБЛЕМА ІДЕНТИФІКАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Швидкий прогрес в розвитку сучасних інформаційних технологій породжує нові виклики і нові ризики, що потребують певного переосмислення загальних засад правового регулювання. В цьому плані останнім часом актуальності набувають специфічні проблеми, пов’язані з використанням Інтернету речей (далі - IP) з елементами штучного інтелекту (далі - ШІ) [1].

Правове регулювання в галузі використання технологічних (в тому числі інформаційних) систем само по собі не є чимось новим. Досі вважалося, що воно поширюється на відносини між людьми, а машина виступала лише як знаряддя в руках людини. Але на наш час починають виникати ситуації, в яких відповідальність лягає саме на машину, незалежно від участі людини [2, 3].

Нагадаємо, що термін «Інтернет речей» на початку означав концепцію впровадження радіочастотних міток в систему керування логістичними ланцюжками [4, 5]. З часом під IoT почали розуміти концепцію обчислювальної мережі фізичних предметів ("речей"), оснащених вбудованими технологіями для їх взаємодії одне з одним або з оточуючим середовищем [6]. Головна ідея полягала в тому, що використання таких мереж дозволить (принаймні, частково) виключити участь людини. На наш час переважає розуміння IoT як сукупності технічних систем і комплексів, що взаємодіють між собою через мережу Інтернет [1, 3]. Вважається, що концепція IoT в практичній реалізації має як технологічні, так і соціальні наслідки [2].

Загрози та ризики, що виникають в сфері використання IP, широко обговорюються в експертному середовищі. Стислий виклад поточного стану речей міститься, наприклад в звітах групи Alliance for Internet of Things Innovation, (AIPI), створеної 2015 року у Європейській Комісії [7].

Особливо складні (і критичні) ситуації у використанні IP-систем виникають у випадках наявності в них елементів ШІ.

В рамках даної доповіді для нас становитиме інтерес здатність машини самостійно приймати рішення. Причому йдеться не про імітацію прийняття рішення

(що на наш час не є чимось особливим), а здатність машини приймати рішення, яке однозначно не визначається набором алгоритмів, обраними значеннями їх параметрів та структурою вхідних даних. Саме така поведінка машини дає підстави говорити про її відповідальність за власні дії, що є предметом правового регулювання. І саме в цьому плані елементи ШІ відіграють ключову роль.

З формальної точки зору, штучний інтелект – це здатність інженерної системи здобувати, обробляти та застосовувати знання та вміння [8]. Крім того, штучний інтелект оцінюється загальною здатністю агента досягати мети в широкому діапазоні середовищ [9].

Для нас важливо те, що за певних умов ШІ дійсно може замінити людину не лише на рівні виконання технічних завдань, але й у прийнятті рішень. В тому числі і таких, що можуть мати негативні наслідки для оточення. І це породжує специфічну проблему, яка, наскільки нам відомо, на даний момент не обговорюється в наявних дискурсах.

Очевидно, що завжди існує якісна відмінність між відповідальністю людини та "відповідальністю" машини. Тому для правильної оцінки відповідальності необхідно точно знати, хто або що має відповідати в кожному конкретному випадку. Іншими словами, ми повинні точно визначити співвідношення ролей людини і машини: до чого саме призвели дії людини, а до чого – дії машини. А для цього, зокрема, необхідно визначити, чи могла дана машина самостійно приймати рішення, тобто чи містить вона елементи ШІ. Отже, маємо проблему ідентифікації ШІ в реальних кібернетичних системах. На перший погляд питання тривіальне, але в дійсності за ним може стояти низка складних питань. Така ситуація виникає, коли ми не маємо точної інформації про будову і функціональні можливості системи.

Наведемо конкретний приклад, який свідчить про те, що проблема перестає носити виключно теоретичний характер. Можливо, питання про його актуальність в сфері ІР є відкритим, але він наочно демонструє практичні аспекти використання ШІ.

За останній час трапилось вже кілька подібних інцидентів, але цей з певних причин набув значного суспільного резонансу. Йдеться про ДТП, що трапилось за участю т. з. "розумного автомобіля". Сьогодні використання ШІ в автомобілебудуванні є надзвичайно перспективнішим напрямом, який активно впливає на відповідний сегмент ринку [10]. Тому такі випадки починають становити інтерес в суто практичному плані.

19 квітня 2021 р. Автомобіль Tesla врізався в дерево, внаслідок чого загинуло двоє людей [11]. За даними поліції в момент аварії за його кермом нікого не було. Тіло одного з загиблих виявили на передньому пасажирському сидінні, другого - на

задньому. На підставі вивчення місця та обставин події поліція дійшла висновку, що "в момент удару ніхто не керував транспортним засобом".

Отже, виникає нетривіальне питання про відповідальність за дане ДТП. Відповідь на нього залежить, в першу чергу, від того, чи можна вважати систему автоматичного керування машини автопілотом, тобто чи могли пасажири повністю покладатися на її роботу без участі людини. Компанія Tesla стверджує, що так. Але з цього приводу існують серйозні сумніви.

Так, рішенням мюнхенського суду визнано, що назва "автопілот" не відповідає дійсності і створює хибне уявлення про можливість самостійного керування автомобілем [12]. Тим самим заохочується небезпечна поведінка, що порушує правильну взаємодію людини з машиною.

Отже, ми бачимо, що в реальному житті виникають ситуації, в яких неможливо однозначно з'ясувати, якою мірою маємо справу з ШІ, тобто де завершується відповідальність людини і починається "відповідальність" машини.

На наш погляд, доцільно було б розробити загальні засади для здійснення експертизи, яка б дозволила з високим рівнем достовірності визначити фактичні функціональні можливості кібернетичної системи, достатні для вирішення питання про ступінь відповідальності машини і людини.

Література:

1. Баранов А. Интернет вещей и искусственный интеллект: истоки проблемы правового регулирования - IT-право. Проблеми та перспективи розвитку в Україні: збірник матеріалів II-ї Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.). Львів : НУ "Львівська політехніка ", 2017. С. 18-42.

2. Рекомендации МСЭ-Т Y.2060 (06/2012). Серия Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений. Структура и функциональные модели архитектуры. Обзор Интернета вещей. URL: http://handle.itu.int/11.1002/1000/11559 (дата звернення 21.04.2021)

3. Баранов О. "Інтернет речей" як правовий термін. Юридична Україна. 2016. № 5-6. С. 96-103. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2016_5-6_16.pdf (дата звернення 21.04.2021).

4. Черняк Л. Платформа Интернета вещей (рус.). Открытые системы. СУБД. 2012. №7. URL: https://www.osp.ru/os/2012/07/13017643/ (дата звернення 21.04.2021)

5. Kevin Ashton. That ‘Internet of Things’ Thing. In the real world, things matter more than ideas. (англ.). RFID Journal. Jun 22. 2009. URL: http://www.rfidjournal.com/articles/view?4986 (дата звернення 21.04.2021)

6.The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment . Gartner IT glossary. Gartner 5 May 2012. URL: https://www.gartner.com/it-glossary/internet-of-things/ (дата звернення 23.04.2021)

7. Charlie Hawes. Hogan Lovells assists Internet of Things policy group in Brussels, 28 October 2015. –Режим доступу : http://www.hlmediacomms.com/2015/10/28/hogan-lovells-assists-internet-of-things-policy-group-in-brussels (дата звернення 23.04.2021)

8. ISO/IEC TR 24028:2020 Information technology - Artificial intelligence - Overview of trustworthiness in artificial intelligence. International Organization for Standardization and International Electrotechnical Commissio (англ.). May 2020.

9. Shane Legg and Marcus Hutter. A Formal Definition of Intelligence for Artificial Systems. URL: http://www.vetta.org/documents/universal_intelligence_abstract_ai50.pdf (дата звернення 23.04.2021)

10. Ильичев В. Умные машины: как искусственный интеллект меняет авторынок https://www.forbes.ru/tehnologii/360953-umnye-mashiny-kak-iskusstvennyy-intellekt-menyaet-avtorynok (дата звернення 23.04.2021)

11. В аварії Tesla загинули двоє людей. За кермом нікого не було https://www.bbc.com/ukrainian/news-56803064 (дата звернення 23.04.2021)

12. Tesla Autopilot ruling a “hazard light on misleading marketing” https://www.thatcham.org/tesla-autopilot-ruling/ (дата звернення 23.04.2021)

Волинчук Юлія
к.е.н., доцент кафедри підприємництва, торгівлі та логістики, Луцький національний технічний університет
Ковальчук Надія
к.е.н., доцент кафедри підприємництва, торгівлі та логістики, Луцький національний технічний університет
Бородавка Катерина
студентка, Луцький національний технічний університет

ІНТЕРНЕТ РЕЧЕЙ ТА WMS-СИСТЕМИ В ЛОГІСТИЧНІЙ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

WMS (англ. Warehouse Management System) – це автоматизована система управління складом), що допомагає автоматизувати всі складські процеси підприємства. Іншими словами, це «програмне забезпечення, яке дозволяє контролювати роботу на складі з моменту щойно прибутого вантажу на склад до моменту завантаження на транспортний засіб» [1]. Як підтверджує практика, впровадження системи WMS є актуальним для тих складських операторів, які відвантажують щонайменше 100-200 вантажів щодня. Погоджуємось, що «сучасні системи управління складом проводять аналітику в режимі реального часу, що дозволяє контролювати всі дії з мінімальною ймовірністю помилок» [2].

При цьому варто зважати на актуальні тенденції, пов’язані з стрімким розвитком цифрових технологій та появою технологій так званого Інтернету речей, що здатний суттєво покращувати результат господарювання підприємств. Зокрема, у виробничих процесах нині широко використовуються бездротові пристрої, що підтримують IP, включаючи смартфони, планшети та датчики. Існуючі дротові сенсорні мережі будуть розширені та доповнені бездротовими мережами у найближчі роки, що значно розширить сфери застосування систем моніторингу та управління на підприємствах. Наступний етап оптимізації виробничих процесів характеризуватиметься все більш щільним зближенням кращих інформаційних та операційних технологій.

Безперечно, «система WMS ефективно працює з технологією Internet of Things: до вантажу прикріплені датчики та контролери, які збирають актуальну

інформацію про стан продукції, умови зберігання та багато інших параметрів. Всі записані дані передаються в систему управління складом» [3].

На першому етапі впровадження встановлюються датчики, виконавчі механізми, контролери та інтерфейси людина-машина. Як результат – з’являється можливість збирати інформацію, що дозволяє керівництву отримувати більш об’єктивні та точні дані про стан виробництва на підприємстві, які в подальшому обробляються і можуть надаватися іншим підрозділам підприємства. Відповідно, цей процес дає можливість налагодити взаємодію між працівниками різних підрозділів та приймати більш ефективні обґрунтовані рішення. Отримані дані можна також використовувати для запобігання позаплановим простоям, поломкам обладнання, зменшенню позапланового технічного обслуговування та збоїв в управлінні процесу поставок, що дозволяє компанії підвищити ефективність як логістичної діяльності, так і компанії в цілому. Складність впровадження цього досвіду пов’язана з тим, що необхідно об’єднати в єдине ціле безліч елементів від різних постачальників та налагодити їх роботу. Ймовірно, це питання часу та лише необхідний крок переходу суспільства до так званого «Інтернету всього» (Internet of Everything).

Література:

1. Сучасні Іт-рішення для управління бізнесом. URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot (дата звернення 26.04.2021)
2. Що таке WMS система або як автоматизувати складську логістику? URL: https://wareteka.com.ua/uk/blog/sho-take-wms-systema/ (дата звернення 26.04.2021)
3. Промисловий Інтернет Речей. URL: https://www.it.ua/knowledge-base/technology-innovation/promyshlennyj-internet-veschej (дата звернення 26.04.2021)

Головко Ольга

к.ю.н.,старший викладач
кафедри публічного права
КПІ імені Ігоря Сікорського

СОЦІАЛЬНЕ ПІДПРИЄМНИЦТВО ТА ТЕХНОЛОГІЇ ІОТ: ПРАВОВИЙ АСПЕКТ

Технології Інтернету речей (далі – IoT) є новим інструментом в межах цифрової трансформації, 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* [1, 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 [2, 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» [2, с. 73]. Це дозволяє зробити висновок, що соціальне підприємництво має три орієнтири: соціальний, ринковий та інноваційний [3].

Таким чином, 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.

Європейський Союз у жовтні 2011 року започаткував ініціативу щодо соціального бізнесу (Social Business Initiative – SBI), спрямовану на створення систем підтримки соціальних підприємств, що впроваджують економічні та соціальні інновації [4]. Соціальне підприємство - це суб'єкт соціальної економіки, основною метою якого є *соціальний вплив*, а не отримання прибутку для своїх власників або акціонерів. Він працює, надаючи товари та послуги для ринку підприємницьким та *інноваційним* способом, і використовує свій прибуток для *досягнення соціальних цілей* [4, с. 2].

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 підприємниць, які взмозі 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 хоча б проблему 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 [5]. 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 даного стартапу стала можливою завдяки:

• чіткому формуванню соціальної мети

• передачі частини доходу на благодійність

• 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. 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.

Дослідження проведено в межах виконання міжнародного проєкту в сфері освіти «European Integration: legislation and the IoT» («Європейська інтеграція: законодавство та Інтернет речей») у межах напряму Жан Моне «Модуль» програми «Erasmus+» №620017-EPP-1-2020-1-UA-EPPJMO-MODULE (спільний проект КПІ ім. Ігоря Сікорського, Еразмус+ Жан Моне Фонду та Виконавчого агентства з питань освіти, аудіовізуальної діяльності та культури за підтримки ЄС)». Підтримка Європейською комісією випуску цієї публікації не означає схвалення змісту, який відображає лише думки авторів, і Комісія не може нести відповідальність за будь-яке використання інформації, що міститься в ній.

Література:

1. Долуда Л., Назарук В., Кірсанова Ю. Соціальне підприємництво. Бізнес-модель. Реєстрація. Оподаткування. Київ: ТОВ «Агентство «Україна». 2017. 92 с.

2. 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.

3. Материалы исследования, проведенного Региональным бюро ПРООН для Европы и СНГ совместно с EMES – Проектом Европейская исследовательская сеть: «Social Enterprise: A new model for poverty reduction and employment generation. An examination of the concept and practice in Europe and the Commonwealth of Independent States». 2008. С. 191.

4. 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: 15.04.2021).

5. Right of reply. URL: https://rightofreply.news/ (дата звернення: 26.04.2021).

Доронін Іван

доктор юридичних наук, доцент
ДНУ «Інститут інформації, безпеки і права
Національної академії правових наук України

ПРАВОВІ ПРОБЛЕМИ ВИКОРИСТАННЯ DL-ТЕХНОЛОГІЙ ДЛЯ ДЕРЖАВНИХ РЕЄСТРІВ

Технологія розподілених реєстрів (*Distributed Ledger Technology*, *DLT*) активно впроваджується у різні сфери людського життя. Не вдаючись в технічні деталі, варто нагадати, що сутність зазначеної технології полягає у відсутності якогось одного фізичного носія інформації (сервера чи системи серверів), що зберігає усю інформацію, або її частину. Інформація, яка зберігається, перебуває одночасно у всіх учасників системи, при цьому жоден з них не контролює ані усю інформацію, ані якусь критично важливу частину.

Із цього випливає можливість доволі тривалого зберігання інформації, особливо захищеної від втрати та модифікації. Такий захист включає і захист від свавільних дій особи, що зберігає інформації або наділена правами на її модифікацію. В умовах постійної компрометації різних видів державних реєстрів в Україні зазначена особливість технології видається цікавою і суспільно потрібною. З огляду на критичну важливість для такої системи проблеми захисту інформації перспективними для прикладного використання поза сферою наукових обчислень є системи, які використовують криптографічний захист і конструювання блоків. Зазначена технологія наразі відома як «блокчейн» (від англомовного терміну *block chain* – ланцюг блоків) і використовується насамперед як розподілена система даних, що закладена в основу «криптовалют» (віртуальних валют, які не мають фізичного аналогу і, як правило, одного емітента), найвідомішою з яких на сьогодні є система «Біткойн».

Пропозиції щодо застосування технології «блокчейн» саме для реєстрів інформації і особливо критичної та важливої інформації є постійними. У вітчизняній науковій літературі зазначена проблема розглядалась з різних боків [1-6]. Після етапу захоплення перевагами технології і намаганням впровадити окремі її прояви в ті, чи інші сфери суспільного життя розпочався період певного охолодження і навіть критики особливо стосовно можливого її застосування саме у сфері державних реєстрів. Річ у тім, що прояв технологій в абсолютному вигляді із застосуванням фактору одночасного розподілу інформації на різних носіях, що не

контролюються, вступає у системне протиріччя із визначенням суб’єкта, відповідального за збереження інформації. Тому, як правило, коли мова йшла про використання DLT для тих чи інших реєстрів застосовувався так званий «приватний блокчейн». Мова йшла про новий рівень захисту інформації. З технічного боку він був значно вищий аніж традиційні засоби захисту інформації. Але навряд чи був економічно і технічного обґрунтованим, оскільки існуючі технічні можливості та відповідна політика користування у принципі створювали і створюють достатній захист від втручання третіх осіб.

Водночас, підвищення рівня довіри до дій державних органів, які визначають політику в сфері реєстрів, а також до дій конкретних уповноважених осіб досі немає. Запропоновані технічні рішення у цій сфері не стосуються захисту інформації в державних реєстрах, оскільки є лише технічними засобами обміну конкретної інформації з них. Слід також зважати і на певну надто захопливість певними технологіями з економічних, рекламних чи політичних міркувань, які до того ж в діях окремих державних органів поєднуються. Якщо всі застосування, котрі згадуються в контексті «держава в смартфоні» є лише засобами обміну конкретної інформації з конкретного реєстру, то слід загадати, що сама чисельність реєстрів та їх адміністрування далекі від ідеалу. Більш того, є багато питань щодо визначення відповідальних саме за інформацію в них. На сьогодні дослідники можуть лише приблизно назвати кількість державних реєстрів та їх адміністраторів. До того ж таке реєстраційне захоплення призвело до виникнення нових суб’єктів – державних підприємств-тримачів реєстрів. Окремі слабкі намагання призвести законодавство щодо реєстрів хоча б до вимог європейських міжнародно-правових актів з питань захисту персональних даних досі не закінчились нічим.

Таким чином основна управлінська (або адміністративна) проблема полягає у неконтрольованому збільшенні:

1) кількості реєстрів;

2) обсягів інформації в реєстрах;

3) кількості суб’єктів адміністрування реєстрами;

4) кількості осіб, уповноважених на здійснення модифікації інформації.

За таких умов відповідальність держави за таку інформацію розмивається.

З огляду на викладене варто повернутись до можливості застосування DLT у деяких галузях, що дотичні до інформації особливо важливої для суспільства. У даному разі таку технологію слід розглядати як гарантію від свавілля. Але на цьому шляху існують певні доволі значні проблеми. До такого проблемного поля належатиме:

– обсяги та межі відповідальності держави за функціонування системи

– визначення стимулів для підтримки функціонування системи користувачами (у випадку «криптовалют» таким стимулом є економічний);

– питання захищеності інформації (насамперед від втрати та спотворення).

Кожний з блоків потребує належної правової регламентації. Так, наприклад, у випадку визначення відповідальності держави важливим вбачається не проста декларація відповідальності держави, а визначення певної політики – від простого та ефективного механізму відшкодування шкоди до зменшення кількості адміністраторів. На першому етапі можливо було б впровадити у повному обсязі та імплементувати у вітчизняне законодавство реально, а не декларативно вимого європейського законодавства у цій сфері.

Література:

1. Konashevych O. The Use of Blockchain Technology for the Development of Electronic Democracy and Electronic Governance. *Часопис Національного університету «Острозька академія», серія «Право»*, 2015. № 1. URL: http://lj.oa.edu.ua/articles/2015/n1/15koiaeg.pdf

2. Доронін І.М. Блокчейн, суспільство і держава: проблеми правотворчості. *ІТ-право: проблеми і перспективи розвитку в Україні: зб. мат. Міжнарод. наук.-практ. конф. (Львів, 17.11.2017) /* НУ «Львівська політехніка». Львів, 2017. С. 73–78.

3. Доронін І.М. Використання сучасних технологій розподіленої обробки даних: право та функції держави. *Інформація і право.* 2017. № 2 (21). С. 51–58.

4. Радейко Р.І. Особливості впровадження технології блокчейн у сфері публічних відносин в Україні. *Часопис цивілістики.* 2018. № 28. С. 112-118.

5. Бакуліна В.О., Сімахова А.О. Блокчейн-технології: світовий досвід та перспективи для України. *Економічні студії*. 2018. № 3. С. 5-10.

6. Bachynskyy, T., Radeiko, R. Legal Regulations of Blockchain and Cryptocurrency in Ukraine. *Hungarian Journal of Legal Studies Acta Juridica Hungarica* Vol. 60 (2019), 1, P. 3-17.

Дубняк Марія

к.ю.н., старший викладач
кафедри інформаційного права та
права інтелектуальної власності
КПІ ім. Ігоря Сікорського

ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В GAME-DEV ІНДУСТРІЇ

Багатомільйонна аудиторія користувачів он-лайн ігор сформувала динамічний ринок стосовно обміну та продажу удосконалених персонажів комп'ютерних ігор або акаунтів. Вартість акаунтів гравців із удосконаленими персонажами може коштувати десятки тисяч доларів, що і породжує проблему законності здійснення вказаних транзакцій. Але питання не скільки у наявності спеціального нормативного акту, скільки в системі права, яка або здатна забезпечити захист прав на цифрові об'єкти або ні.

У даній публікації ми будемо досліджувати чи можуть технології блокчейну вирішити проблеми захисту інтересів гравця у разі обміну (продажу) прав на акаунт у грі, проблему крос-платформенного обміну ресурсами, проблему підтвердження (доведення), що в акаунті дійсно було здобуто ігрові ресурси, ігрову валюту та ігрові артефакти.

Існує ряд проблем пов'язаних з індустрією комп'ютерних ігор: визначення правового режиму акаунту (як в он-лайн іграх, так і в соціальних мережах); визнання права користувача розпоряджатись правами доступу до персонажів (в частині їх продажу) та акаунту гравця у грі (в частині передання прав доступу іншій особі), адже формально відносини між користувачем конкретної гри та студією розробником комп'ютерної гри визначені в ліцензійній угоді користувача (англ. - ELUA — End User Licence Agreement) та Правилах користування (англ. - Terms of Use), які, в більшості випадків, забороняють такі дії.

Однак, наявність попиту, який формують самі користувачі гри, не означає, що гравці будуть належним чином дотримуватись погоджених заборон, визначених в ELUA або Terms of Use. Відтак, між гравцями складаються відносини, які пов'язані із удосконаленням персонажів і продажу акаунту, перепродажу внутрішньоігрових цінностей (артефактів, чи внутрішньоігрових монет), відносини, пов'язані із допомогою у проходженні певного рівня гри та інші. Але Правилами гри

встановлено, що у разі, якщо студія розробник виявить вказані дії по відношенню до акаунтів — вона може їх безповоротно заблокувати. У такому разі у гравців не виникає права на поновлення доступу до акаунту.

З правової точки зору, надання гравцям за плату можливості використання додаткового функціоналу гри (з метою полегшення ігрового процесу, або більш швидкого розвитку персонажа) є самостійною послугою при організації ігрового процесу. Такі відносини розглядаються за правилами встановленими для ліцензійних договорів, в яких доступ до акаунту та ігрового світу це надання права на використання комплексного об’єкту прав інтелектуальної власності, майнові права на який, в цілому, належать студії-розробнику комп’ютерної гри, а сплата коштів — це ліцензійний платіж.

З іншого боку, до таких відносин можна застосувати положення договорів про надання послуг, при цьому жодних прав на акаунт не виникає взагалі, адже “послуга споживається в момент її надання” [1].

Якщо аналізувати Правила гри студії Wargaming, то в них сказано: “Wargaming вправі без попереднього повідомлення користувача змінювати на свій розсуд технічні та інші характеристики будь-якій частині гри, включаючи цифрові товари; змінювати сценарії роботи гри, включаючи зміни ігрового процесу тощо”. Отже, перелік можливих односторонніх змін характеристик гри відкритий.

“Wargaming вправі в будь-який час розірвати угоду в односторонньому позасудовому порядку: у разі закриття Ігри з припиненням можливості використовувати Гру, включаючи цифрові товари, а також інші складові Ігри або у разі будь-якого, в тому числі одноразового, порушення користувачем умов угоди або ключових документів; а також умов використання інших ігор Wargaming”. У цьому випадку Wargaming не повертає користувачеві кошти і не відшкодовує збитки.

При цьому, Wargaming не зобов'язаний надавати користувачеві докази, що свідчать про порушення користувачем умов угоди, в результаті якого користувачеві було припинено або обмежено доступ [2].

Таким чином, ми бачимо, наступне суспільне протиріччя: гравці не можуть отримати доступ до гри без прийняття вказаних Правил. А у разі прийняття Правил, вони не можуть задовольнити свій ігровий інтерес з використанням додаткових послуг — адже Правилами це заборонено.

З правової точки, зору студія-розробник гри у разі виявлення порушення Правил має всі підстави для блокування акаунту гравця.

Також, у Правилах гри існує ряд заборон щодо крос-платформенного використання ігрового акаунту (витративши 300 годин на удосконалення акаунту в

одній грі, ви не можете його використати в іншій, навіть якщо ігровий процес подібний і гра належить тій самій студії. Гравцю все потрібно починати з початку).

Якщо розглядати акаунт гравця як інформаційний ресурс у якому містяться дані про наявні активи (ігрові ресурси, валюту, ігрові артефакти для персонажу) то вказані дані зберігаються на серверах розробника, і у випадку зникнення певних активів з акаунту, гравець не має шансів довести їх наявність.

Отже, постає проблема: як у даному випадку захистити інтереси гравця, зберегти самодостатній ринок послуг щодо продажу удосконалених персонажів та акаунтів, і не втратити права доступу до акаунту і самої гри.

Якщо використати технологію блокчейн для запису даних усього процесу проходження гри, ми отримаємо реєстр усіх транзакцій, які пов’язані із удосконаленням і розвитком персонажа, здобутими ресурсами, які обліковуються в акаунті кожного гравця. При цьому у разі обміну такими ресурсами між гравцями, записи про перехід вказаних одиниць також будуть доступні у реєстрі блокчейну. Поєднання ігрової індустрії та блокчейн технологій може забезпечити реальну можливість підтвердження прав (або приналежності цифрових об’єктів) конкретним особам. Отже, витрачені фіатні кошти на удосконалення персонажа, або десятки годин на його розвиток не будуть витрачені бездоказово. Зникає суб’єкт, який в односторонньому порядку може змінювати правила гри, здійснювати блокування акаунтів та нівелювати цінність ігрових артефактів.

Висновки: використання блокчейн технологій в ігровій індустрії може вирішити три проблеми щодо захисту інтересів гравців: проблему підтвердження прав на акаунт і удосконаленого персонажа комп’ютерної гри, проблему крос-платформенного обміну, проблему підтвердження даних про те, скільки і яких ресурсів здобув гравець у грі. Оскільки, завдяки застосуванню блокчейн технологій записи про вчинені дії під час ігрового процесу зберігаються децентралізовано, у всіх учасників гри, і не підлягають односторонній зміні чи вилученню.

Література:

1. Цивільний кодекс України : Кодекс України № 435-IV від 16.01.2003. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

2. Wargaming.net products & services: Legal documentation URL: https://legal.eu.wargaming.net/en

Закірова Світлана
кандидат історичних наук, доцент,
старший науковий співробітник,
Національна бібліотека України
імені В. І. Вернадського

ОНОВЛЕННЯ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЗА ПРИНЦИПАМИ ЄВРОПЕЙСЬКИХ СТАНДАРТІВ

Яскравою прикметою сучасного життя є використання електронних засобів комунікації. Причому якщо раніше зв’язки за допомогою сучасних технологій були поширені лише в окремих країнах, то сьогодні діджиталізованими контактами з різним ступенем якості охоплені усі без винятку регіони світу. За даними міжнародних аналітиків, у 2020 р. 4,8 мільярда людей у світі користувалися Інтернетом, що становить біля 63 % населення. Регіоном із найбільшою чисельністю користувачів Інтернету у світі (біля третини загальної кількості) є Азія (2,5 мільярда), де провідні ролі відіграють дві держави – Китай (934 мільйони) та Індія (697 мільйонів). Натомість саме у цих країнах також і найбільша кількість осіб, які не мають доступу до всесвітньої мережі. Друге місце за кількістю користувачів посідає Європа (727,8 мільйони). Найбільш стрімко (понад 80 % порівняно з 2015 р.) зростає чисельність користувачів Інтернету в Африці (556 мільйонів). За прогнозами експертів до 2025 р. 5,6 мільярдів жителів стануть користувачами всесвітньої мережі [1].

Утім великі переваги і можливості, що надає людству доступ до Інтернету, несуть із собою збільшення ризиків і появу нових загроз, пов’язаних із кіберзлочинністю та крадіжкою персональних даних громадян. Небезпека цих видів правопорушень суттєво підсилюється можливостями дистанційного скоєння незаконних дій, через що злочинці фізично можуть знаходитися далеко від особи, проти якої спрямовані їх дії. Відтак питання боротьби з порушеннями прав у сфері захисту персональних даних є вкрай важливим як на національному, так і на глобальному рівнях.

Захист персональних даних в Україні регулюється відповідним законом (2011 р.), до якого неодноразово вносили зміни та доповнення. Ст. 11 закону «Про захист персональних даних» встановлює вичерпний перелік підстав обробки персональних даних. Ключовою з таких підстав є згода суб’єкта персональних

даних і, за виключенням окремих випадків, саме наявність згоди є обов’язковою умовою збору персональних даних в Інтернеті.

Відповідно до ст. 22 чинного закону функцію контролю із захисту персональних даних в Україні покладено на Уповноваженого Верховної Ради України з прав людини і судові органи. У структурі Секретаріату Уповноваженого Верховної Ради України з прав людини працює спеціальний Департамент у сфері захисту персональних даних. Проте за своєю природою Уповноважений є медіатором, а не каральним органом і не може безпосередньо накладати санкції. На підставі проведених омбудсменом перевірок рішення про накладання санкцій ухвалюють суди, що значно уповільнює процес притягнення до відповідальності порушників [2].

За даними представника Уповноваженого Верховної Ради з прав людини у сфері захисту персональних даних І. Берназюк у 2020 р. до Уповноваженого надійшло понад 2 000 скарг про порушення прав людини, що майже удвічі більше ніж у 2019 р. За її словами, звернення стосувалися порушень прав людини через втручання в сімейне та особисте життя під час здійснення колекторської діяльності; незаконного поширення персональних даних через мережу Інтернет; неправомірного витребування згоди на обробку персональних даних у тих випадках, коли вона не потрібна; поширення персональної інформації у месенджерах і соціальних мережах; порушення під час впровадження електронних сервісів тощо [3].

Утім попри велику кількість звернень про порушення законодавства у сфері захисту прав людини до суду потрапляють одиниці справ. Зокрема, з 1 061 звернення до Уповноваженого у 2019 р. апаратом омбудсмена складено і направлено до суду лише 10 протоколів про адміністративне правопорушення. Такий результат в офісі омбудсмена пояснюють тим, що законодавством обмежені строки притягнення до відповідальності (3 місяці з дня вчинення), а звернення здебільшого надходять до секретаріату Уповноваженого вже після пропущення строків [5].

Захист персональних даних громадян виступає одним із пріоритетів діяльності і Міністерства цифрової трансформації України. За словами заступниці профільного міністра Л. Рабчинської, суттєвою проблемою, яка ускладнює можливості такої роботи, є відсутність механізму видалення персональних даних з мережі, невизначеність окремих питань обробки біометричних даних.

З метою осучаснення українського правового поля у березні 2021 р. було презентовано новий законопроєкт «Про захист персональних даних», що складається з 10 розділів і 71 статті. Документом передбачається оновлення принципів обробки персональних даних, запровадження чіткого регулювання їх

захисту та осучаснення термінів у законодавстві. Прийняття сучасного законодавства у сфері електронних комунікацій відповідає загальній стратегії інтеграції України до єдиного цифрового ринку Європейського Союзу, що передбачає формулювання і приведення у відповідність до правил ЄС принципів обробки персональних даних, положення про їх вільний рух.

Особливо актуальним виглядають міжнародні зобов'язання України, враховуючи те, що і європейське законодавство останнім часом суттєво оновилося. У зв'язку з прийняттям у 2018 р. Регламенту в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони (GDPR) вимоги до опрацювання персональних даних стали значно суворішими. Навіть в умовах стрімкого поширення світом пандемії короновірусної хвороби COVID-19 європейське законодавство (Конвенція 108, Модернізована Конвенція 108+, GDPR) гарантує високі стандарти у сфері захисту персональних даних. Зокрема, у спільній заяві Комітету Конвенції 108 та Уповноваженого Ради Європи із захисту даних від 30 березня 2020 р. наголошується, що Модернізована Конвенція 108+ визнає необхідність допущення деяких винятків та обмежень задля нагальних цілей, які є життєво важливими та становлять суспільний інтерес. Проте, такі обмеження мають відповідати чітким вимогам з метою забезпечення безперебійного дотримання верховенства права [4, с. 408].

Дещо інакше ситуація розвивається в Україні. Так, прийнятий у квітні 2020 р. Закон України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)», фактично дозволяє збирати, систематизувати, обробляти персональні дані фізичних осіб без їх згоди. І хоча в документі зазначається, що використання таких даних допускається виключно з метою здійснення протиепідемічних заходів і в порядку встановлення карантинних обмежень, на практиці такі новації можуть спричинити неправомірне використання особливо чутливої для особи інформації про стан її здоров'я.

Практика підтверджує, що захист персональних даних громадян ЄС суттєво відрізняється від українських реалій не тільки нормативною базою, але й можливостями їх ефективного захисту. В європейських країнах органи контролю за правомірним використанням персональних даних мають значно ширші повноваження, ніж в Україні. Важливим аспектом діяльності у сфері захисту персональних даних в Європі є можливість прямого притягнення до відповідальності не тільки окремої людини, але й великих гравців на ринку послуг. Наприклад, у 2020 р. шведський орган управління захисту даних (DPA) наклав

штраф у розмірі 75 мільйонів шведських крон (приблизно 7 мільйонів євро) на Google як оператора пошукової системи за невиконання вимог GDPR щодо вилучення персональних даних через неточність або оскільки така інформація була зайвою [5]. Натомість в українських судах справи про накладання санкцій на порушників законодавства щодо використання персональних даних практично відсутні.

Тож для підвищення ефективності захисту прав громадян у новому законопроекті передбачається створення спеціального органу, який матиме повноваження самостійно накладати санкції за неправомірну діяльність у сфері розповсюдження персональних даних. І хоча для функціонування цього органу додатково розробляється окремий законопроект, у вже оприлюдненому документі закладено важливі функції контролюючого органу накладати штрафи за порушення у сфері захисту персональних даних. У випадку ухиляння порушника від сплати штрафу питанням його стягнення будуть займатися виконавчі служби.

Разом з тим, необхідною складовою боротьби в Україні з порушеннями прав на захист персональних даних є підвищення загального рівня правової культури громадян. Як свідчать дані Єврокомісії, після прийняття GDPR і проведення відповідної інформаційної кампанії показник тих, хто точно знали про рівень відповідальність за невиконання регламенту у сфері захисту персональних даних і готові свідомо захищати свої права, зріс на 20 %.

Отже, шляхом для підвищення ефективності захисту персональних даних в Україні має стати не тільки прийняття нового законодавства, що відповідає сучасним європейським і світовим стандартам, але й наполеглива робота з формування у громадян і відповідних органів високої правової культури Інтернет-комунікації та відповідального ставлення до персональних даних і системи їх захисту.

Література:

1. Global Digital Population Grows to 4.8B in 2020 (2020). *TV Tech.* URL: https://www.tvtechnology.com/news/global-digital-population-grows-to-48b-in-2020

2. Правдиченко, А. (2019). Персональні дані онлайн: проблеми регулювання та перспективи захисту. *Центр демократії та верховенства права*. URL: https://cedem.org.ua/articles/personalni-dani-onlajn/

3. Посилення законодавчого забезпечення захисту персональних даних в Україні обговорено під час круглого столу у Верховній Раді (2021). *Верховна Рада України. Офіційний вебпортал парламенту України.* URL: https://www.rada.gov.ua/news/news_kom/205937.html

4. Калітенко, О. (2020). Окремі проблеми захисту персональних даних в умовах COVID-19. *Правове життя сучасної України*. *Матеріали Міжнар. наук.-практ. конф.* Т. 3, 407-410.

5. Матола, В. (2020). «Баги» державних реєстрів, або як захистити персональні дані. *LB.ua*. URL: https://lb.ua/pravo/2020/05/19/457892_bagi_derzhavnih_reiestriv_abo_yak.html

Колодій Інна

кандидат юридичних наук, доцент,
зав. кафедри цивільного, господарського
права та процесу Національного
університету «Чернігівська політехніка»

«ПРАВО НА ЗАБУТТЯ» ЯК СПОСІБ ЗАХИСТУ ПРАВА НА ПРИВАТНІСТЬ В МЕРЕЖІ ІНТЕРНЕТ: РЕАЛІЇ ТА ПЕРСПЕКТИВИ

Глобалізаційні процеси, які пришвидшеними темпами відбуваються у світі, тісно пов’язані з розвитком феномену інформатизації, у зв’язку з чим все більшої резонансності набуває право кожного на захист персональних даних. Стандартом сьогодення стає ситуація, за якої в мережі Інтернет поширюється інформація, що порушує право на приватність, оскільки є неправдивою, або вже не актуальною. Саме право на захист персональних даних охоплюється низкою суб’єктивних прав, які по-різному закріплені в законодавстві окремих держав, що фактично призводить до юридичних проблем на міжнародному рівні.

Важливим елементом права на приватність в мережі Інтернет є «право на забуття» чи «право бути забутим» (*анг. Right to be forgotten*), зміст якого передбачає можливість особи вимагати видалення даних про себе, чи інформації, актуальність якої втрачена, але Інтернет її пам’ятає та надає до неї доступ. Реалізація особами зазначеного права на сьогодні розцінюється як суттєвий прорив у розвитку інформаційних і правових технологій, хоча низка проблем на практиці виникає.

Стаття 7 Хартії основних прав Європейського Союзу проголошує, що «кожна людина має право на повагу її особистого та сімейного життя, на недоторканість житла та таємницю кореспонденції». В статті 8 про захист даних особистого характеру зазначено: «Кожна людина має право на охорону даних про неї особистого характеру. Ці дані повинні використовуватися у відповідності із

встановленими правилами у визначених цілях і на основі дозволу заінтересованої особи або на інших правових підставах, передбачених законом. Кожна людина має право на доступ до зібраних даних, які її стосуються, і право на внесення до них змін» [1]. Директива ЄС 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [2] стала прообразом застосування цих прав.

В 2016 році на зміну Директиві 95/46/ЄС було прийнято Регламент 2016/679 «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних», ст. 17 «Право на стирання («право бути забутим»)» та ст. 21 «Право на заперечення» якого закріплюють право суб'єкта даних вимагати стирання персональних даних, що його стосуються, і відповідний обов'язок стирати ці дані з боку контролера даних у випадку, якщо суб'єкт даних заперечує проти обробки даних і відсутні легітимні підстави для такої обробки, які переважають над інтересами, правами та свободами суб'єкта даних [3].

При реалізації «права бути забутим» на практиці часто виникають проблеми щодо того, хто має виступати в якості контролера даних у якості розуміння законодавства Європейського Союзу. Пошукові системи на сьогодні є надзвичайно впливовими суб'єктами відносин в мережі Інтернет і тому не «прагнуть» брати на себе зобов'язання з видалення інформації, акцентуючи на тому, що вони є звичайними посередниками між користувачами та веб-сайтом; не створюють інформацію, яка виступає предметом спору, а «контент», який вони продукують це лише підбір та порядок посилань у відповідь на запит.

Переслідуючи мету знайти відповідь на це питання, вважаємо за необхідне звернутись до практики Європейського суду з прав людини (ЄСПЛ), який в окремих справах досліджував необхідність видалення даних, які з часом втратили свою актуальність. Так, у рішенні ЄСПЛ по справі «Google Spain SL, Google Inc. проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса», заява № C-131/12 від 13 травня 2014 року, перед ЄС було порушено питання, чи потрібно компанії Google видалити з результатів пошуку посилання на інформацію щодо продажу будинку через аукціон у 1998 році, розміщену на веб-сайті однієї з іспанських газет. Компанія Google заперечувала свою відповідальність, зазначаючи, що вона лише надає гіперпосилання на веб-сайт, де розміщено інформацію і вимога щодо видалення має бути направлена до адміністратора веб-сторінки, а не до Google, яка лише надає посилання на сторінку-першоджерело. ЄСПЛ дійшов висновку, що Google під час пошуку в мережі інформації та веб-сторінок, а також індексування змісту для надання результатів пошуку, стає контролером даних, на

якого покладається відповідальність та зобов’язання відповідно до законодавства ЄС.

ЄСПЛ у своєму рішенні роз’яснив, що пошукові системи мережі Інтернет та результати пошуку, що надають персональні дані, можуть створити детальний профіль фізичної особи. Окрім того, пошукові системи надають інформації, що знаходиться в переліку результатів пошуку, характеру повсюдності. Зважаючи на потенційну небезпечність, таке втручання не може бути виправдане лише економічним інтересом оператора відповідної системи в такій обробці. Необхідно досягнути справедливого балансу, зокрема, між легітимним інтересом Інтернет-користувачів у доступі до інформації та фундаментальними правами суб’єкта персональних даних, передбаченими ст. 7 та ст. 8 Хартії основних прав ЄС.

Вирішуючи питання, чи необхідно було Google видалити посилання, які стосувалися заявника, Суд вважав, що за певних обставин фізична особа має право вимагати видалення персональних даних (у випадку якщо інформація щодо фізичної особи неточна, неадекватна, невідповідна або надмірна щодо цілей обробки персональних даних). Суд визнав, що це право не є абсолютним, та має бути встановлено баланс між ним та іншими правами та інтересами, зокрема з інтересом громадськості щодо доступу до певної інформації. Будь-яка вимога видалення даних має підлягати оцінці в кожному окремому випадку шляхом встановлення балансу між основоположними правами на захист персональних даних і приватного життя суб’єкта даних, з одного боку, та легітимними інтересами всіх Інтернет-користувачів, - з іншого.

ЄСПЛ надав вказівки щодо факторів, які мають бути враховані під час знаходження такого балансу. Характер відповідної інформації є особливо важливим фактором, тобто якщо інформація стосується приватного життя фізичної особи, при цьому суспільний інтерес до неї відсутній, захист персональних даних і приватне життя переважатиме над правом громадськості на доступ до інформації, і, навпаки, якщо виявиться що суб’єкт даних є публічною особою або характер запитуваної інформації виправдовує її доступність для широкої громадськості, переважний суспільний інтерес щодо доступу до інформації може виправдати втручання в основні права на захист персональних даних та приватне життя суб’єкта даних [4].

Стосовно територіального доступу до оспорюваного контенту, то дія Регламенту поширюється на всіх суб’єктів, які здійснюють обробку персональних даних громадян та компаній ЄС, незалежно від їхньої територіальної приналежності. У рішенні ЄС по справі «Google LLC v. CNIL (Національна комісія з інформатики та свободи)» від 24 вересня 2019 року Суд постановив, що пошукова система має дотримуватись права на забуття у межах території Європейського

Союзу [5]. У рішенні по справі «Eva Glawischnig-Piesczek v. Facebook Ireland Limited» від 3 жовтня 2019 року, Суд ЄС дійшов висновку, що у випадку, якщо поширений у мережі контент попередньо визнаний національним судом таким, що містить про особу недостовірну інформацію, Facebook повинен накласти повне обмеження доступу до такої інформації по всьому світу. Також згідно з рішенням суду, пошукові системи зобов'язані вжити заходів, щоб користувачі в країнах ЄС не могли перейти по посиланню на сайти, які не відповідають європейському законодавству [6].

Таким чином, рішення ЄСПЛ має на меті не захист осіб від негативної публічності в Інтернет (а інформація негативного та неправдивого характеру неодмінно призводить до негативної публічності), а їх захист від давньої інформації, що є неточною, неадекватною, невідповідною або надмірною щодо цілей обробки персональних даних. Відповідно, у кожному поданому позові необхідно обґрунтувати, що інформація яка розміщена в мережі Інтернет має характер неточної, неадекватної, невідповідної або надмірної щодо цілей обробки персональних даних, та відповідно результат справи залежатиме від обґрунтованості поданого позову.

Виникнення правового інституту «права на забуття» слід розглядати як закономірний етап розвитку глобалізованого правового інформаційного простору. «Право на видалення даних» виступає в якості своєрідного способу захисту права на приватність в мережі Інтернет, а його закріплення у вітчизняному законодавстві сприятиме забезпеченню високого рівня захисту персональних даних.

Література:

1. Хартія основних прав Європейського Союзу від 07.12.2000 р. URL: https://zakon.rada.gov.ua/laws/show/994_524.

2. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 25.10.1995 р. (скасована на підст. Регламенту № 2016/679 від 27.04.2016 р.). URL: https://zakon.rada.gov.ua/laws/show/994_242.

3. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» від 27.04.2016 р. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#top.

4. Рішення по справі «Google Spain SL, Google Inc. проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса», № C-131/12 від 13.05.2014 року. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

5. Рішення по справі «Google LLC v. CNIL (Національна комісія з інформатики та свободи)», № C-507/17 від 24.09.2019 року. URL: https://curia.europa.eu/juris/document/document.jsf?text=erasure&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2938101#ctx1.

6. Рішення по справі «Eva Glawischnig-Piesczek v. Facebook Ireland Limited», № C-18/18 від 03.10.2019 року. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6039379.

Костенко Олексій

Ph.D. в галузі права,
в.о. завідувача науково-дослідної
лабораторії теорії і права цифрових
трансформацій науково-дослідного центру
цифрових трансформацій і права
ДНУ «Інститут інформації, безпеки і права
Національної академії правових наук України»

ІДЕНТИФІКАЦІЙНІ ДАНІ IoT: ПРОБЛЕМИ ФОРМУВАННЯ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ПРИ ЗАСТОСУВАННІ ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ

Інтернет речей нині є невід’ємним атрибутом повсякденного життя. Індустрія пристроїв Інтернету речей (IoT) стрімко зростає. Постійно збільшується перелік компаній-виробників, які пропонують для застосування безліч сучасних розумних пристроїв IoT, з метою покращення різних сфер життєдіяльності людини. Існує широкий спектр нових додатків IoT, що збирають різноманітні дані та керують процесами і об’єктами.

На сьогодні до мережі Інтернет підключено мільйони IoT-пристроїв і число таких пристроїв збільшується щодня. У більшості користувачів цих IoT-пристроїв існує уява стосовно технічної та юридичної захищеності під час їх застосування. В той же час виробники пристроїв IoT не переймаються стосовно можливих негативних наслідків, які створюють їх вироби із попередньо встановленими іменами користувачів та паролями, з включеними мережевими сервісами, які не потрібні для даних продуктів, а також великою кількістю вразливостей,

виправлення для яких у вигляді оновлення програмного забезпечення з’являються дуже рідко і з великою затримкою, або взагалі їх немає. Це призводить до інцидентів, таких як, наприклад, DDoS-атака ботнета Mirai, яка вразила мільйони пристроїв IoT [1].

Слід зауважити й на те, що сучасне IoT середовище неоднорідне в механізмах і схемах ідентифікації пристроїв та їх користувачів. Так, для передачі даних пристрої IoT застосовують такі радіотехнології, як LoRaWan, LTE-M, Sigfox, NB-IoT, NFC BLE, Wi-Fi, Z-Wave, ZigBee. Одні, такі як Zigbee, BLE, WiFi, мають малу дальність дії, інші, як 3G і LTE, мають проблеми енергоспоживання і нестабільний радіус або сектор радіопокриття [2].

До відомих платформ IoT відносяться: Amazon Web Services, Microsoft Azure, ThingWorx IoT Platform, IBM’s Watson, Cisco IoT Cloud Connect, Salesforce IoT Cloud, Oracle Integrated Cloud, GE Predix [3].

Ідентифікатори стандарту IoT сьогодні прийнято розділяти на категорії:

- ідентифікатори об’єктів, які використовуються для ідентифікації фізичних або віртуальних об’єктів (URIs, URL);
- ідентифікатори зв’язку, які застосовуються для унікальної ідентифікації пристроїв у межах комунікації з іншими пристроями, включаючи Інтернет-зв’язок (IPv4, IPv6, E.164);
- ідентифікатори додатків, які визначають унікальні програми, що використовуються в межах IoT додатків (EPC, UPC, Handle/DOI, UUID, MAC, URI, URL, Ecode, OID, CID) [4].

Існують різні універсальні ідентифікаційні системи, такі як Object IDentifier (OID), електронний код продукту (EPC), універсально-унікальний ідентифікатор IDentifier (UUID), міжнародний ідентифікатор мобільного обладнання Identity (IMEI) тощо [5].

Різноманітність підходів ідентифікації відзначається і серед технічних стандартів, рішень безпеки та платформ сумісності IoT - «M2M», «GS1», «OCF» та «FIWARE», FIDO та AIOTI. Проект FIDO Alliance (Fast IDentity Online) розробляє стандарти WebAuthn і CTAP, які будуть основою для різноманітних методів безпарольної автентифікації: біометричної, голосової, 2D- 3D- фото, одноразових паролів та USB-ключів.

Отже, сучасні технології IoT досить стрімко розвиваються. В той же час, існує суттєве відставання законодавства в реагуванні на розвиток суспільних відносин із використанням технологій та пристроїв IoT. Досі відсутні єдині підходи до юридичного оформлення нормативної бази в цій галузі. Крім того, немає одностайної наукової думки щодо деталізації та однозначності формулювання

дефініцій в даній сфері. Саме на цю обставину звертають увагу в своїх дослідженнях Світовий банк та Комісія Організації Об’єднаних Націй з права міжнародної торгівлі, ЮНСІТРАЛ (UNCITRAL).

Також суттєвим ускладненням для управління ідентифікаційними даними пристроїв IoT є відсутність єдиного класифікатора ідентифікаційних даних. Таким чином невизначеності додає й низка різних схем ідентифікації суб’єктів за ідентифікаційними даними. Так, наприклад, тільки в Україні офіційними вважаються п’ять схем: «QsignID», «BankID», «MobileID» «PasscardID» та «ДіяID».

Наразі існує достатньо багато напрямів вирішення проблеми ідентифікації пристроїв IoT. Так, наприклад, метод ідентифікації пристроїв IoT на основі ентропії їх застосування в різних мережевих умовах [6]; метод ідентифікації та класифікації IoT, заснований на алгоритмах машинного навчання, що аналізують статичну та динамічну поведінкову модель пристроїв [7]; створення системи ідентифікації подібної до структури ДНК, заснованої на статичних атрибутах пристроїв IoT [8]; створення єдиного класифікатора пристроїв IoT в системі класифікації ідентифікаційних даних суб’єктів та об’єктів інформаційних систем [9]; метод із застосуванням пристроїв IoT, які мають сертифікати з цифровим підписом, що технічно і фізично неможливо вилучити із пристрою.

Сьогодні формування суспільних відносин відбувається під впливом четвертої науково-технічної революції із масштабним застосуванням інформаційно-комунікаційних технологій та мережі Інтернет. Традиційні суспільні відносини достатньо ґрунтовно врегульовані правовими нормами, інститутами та галузями права. Водночас суспільні відносини в сфері застосування пристрів IoT залишаються неврегульовані. Існуючі нині закони не сформульовано з урахуванням можливої появи цифрових технологій застосування пристроїв IoT, які не розглядають питання нормативної регуляції в даній сфері та неналежним чином застосовують застрілі норми права до багатьох нових суспільних відносин. Також нормативно-правові акти можуть регулювати певні питання застосування пристроїв IoT, як технічних пристроїв. Однак сфера їх застосування часто базується на принципі двозначності, що призводить до виникнення ситуації правової невизначеності.

На нашу думку зараз нагальною потребою науковців та правознавців є формування сучасної та загально прийнятної юридичної термінології в сфері IoT, а також створення єдиного та сталого бачення правових проблем, єдиного підходу в правовому регулюванні на національному та міждержавному рівні, особливо в тій частині застосування пристроїв IoT, які задіяні в нейро/кардіо- медицині, військовій техніці та зброї, на об’єктах критичної інфраструктури, виведення з ладу або

порушення функціонування яких може становити потенційну загрозу життю і здоров’ю людей.

Застосування пристроїв та технологій IoT формують нову електронну екосистему, що кардинально змінює відношення людства до результатів науково-технічної революції, а також ставлення особистості до процесів пізнання та сприйняття цифрової реальності, можливостей відтворення «віртуальної людини» за допомогою пристрів IoT та штучного інтелекту.

Темпи цифровізації суспільних відносин спонукають нормотворців та правознавців до активної модернізації законодавства, яке в сфері управління ідентифікаційними даними є архаїчним та мало розвинутим.

Інтеграція України в світові цифрові ринки та транскордонні електронні відносини повинна відбуватись одночасно із трансформацією національного законодавства із врахуванням передового світового досвіду в галузі управління ідентифікаційними даними.

Література:

1. Ботнет Mirai: защиты нет и не предвидится. URL:https://networkguru.ru/botnet-mirai/(дата звернення: 07.04.2021).

2. Интернет вещей: LoRa устройства от Mikrotik // Lanmarket. – 2019. – URL: https://lanmarket.ua/stats/internet-veshchey-lora-ustroystva-ot-mikrotik/(дата звернення: 29.03.2021).

3. Что такое IoT, или интернет верей // coinspot.io – 2016. – URL: https://coinspot.io/beginners/chto-takoe-iot-ili-internet-veshhej. (дата звернення: 19.03.2021).

4. Internet of ThingsEU-China Joint White Paper on Internet-of-Things Identification European research cluster on the Internet of things // European Communities, 2015. Reproduction authorised for non-commercial purposes provided the source is acknowledge. – 2015. – URL: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_EU-China_IoT_Identification_Final.pdf. (дата звернення: 11.01.2021).

5. Костенко О.В. Ідентифікація IoT: витоки проблеми правового регулювання управління ідентифікаційними даними. Juris Europensis Scientia № 1/2021. С.112-119.

6. Bruhadeshwar Bezawada, Maalvika Bachani, Indrajit Ray. Behavioral Fingerprinting of IoT Devices. – URL: https://www.researchgate.net/publication/328323796_Behavioral_Fingerprinting_of_IoT_Devices. DOI:10.1145/3266444.3266452/(дата звернення: 29.03.2021).

7. Entropy-based IoT Devices Identification. Hung Nguyen An Thomas Silverston Taku Yamazaki Takumi Miyoshi. – URL:
https://www.researchgate.net/publication/346378679_Entropy-based_IoT_Devices_Identification DOI:10.34385/proc.62.TS4-1/(дата звернення: 29.03.2021).
8. Nancy Scheidt Mo Adda.Identification of IoT Devices for Forensic Investigation. – URL: https://www.researchgate.net/publication/338677729_Identification_of_IoT_Devices_for_Forensic_Investigation DOI:10.1109/IS48319.2020.9200150/(дата звернення: 29.03.2021)
9. Kostenko O.V. Identification data management: legal regulation and classification. «PNAP». Scientific Journal of Polonia University Periodyk Naukowy Akademii Polonijnej. Том 43 № 6 / 2020. P.212-220.

Солончук Ірина
старший викладач кафедри
інформаційного права та права
інтелектуальної власності
КПІ ім. Ігоря Сікорського

ЦИФРОВА ТРАНСФОРМАЦІЯ: ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ (IoT) У СФЕРІ СУДОЧИНСТВА

Цифрова трансформація суспільних відносин, а саме впровадження технологій Інтернету речей у різних сферах діяльності, викликана об’єктивними закономірностями розвитку соціуму. За висновком О. А Баранова технології Інтернету речей мають потенційні спроможності забезпечити прийняття рішень, які будуть максимально адекватними поточній ситуації в суспільних процесах завдяки можливості в режимі реального часу збирати та обробляти значні обсяги інформації (дані), зокрема інформацію щодо великої кількості об’єктів та суб’єктів, які задіяні в таких процесах, а також приймати чи пропонувати рішення, які виробляються на основі спеціальних математичних алгоритмів, зокрема алгоритмів штучного інтелекту [1, с. 42-43].

Штучний інтелект, який впроваджується та активно використовується у різноманітних видах суспільної діяльності, не лише значною мірою полегшує

виконання визначених функціональних завдань, але і потребує детальної уваги науковців, зокрема представників правової науки з метою вдосконалення врегулювання даних правовідносин. Наразі вимоги життя такі, що соціальні зміни потребують негайної реакції законодавця у питанні правової визначеності конкретних процесів з метою їх врегулювання. У зворотному випадку не уникнути проблем, суперечностей та конфліктів. Виконавши аналіз публікацій останніх років, присвячених Інтернету речей, погоджуємося із науковою думкою, що проблемою сучасної правової науки є відсутність єдності дефініцій термінів, які виникли в результаті науково-технічного прогресу та пов’язані з використання технологій ІР. Правова наука завжди вимагає визначеності та упорядкування термінологічного апарату. Технологічні революції спровокували появу технократичних термінів, які згодом стали активно використовуватися в праві. В даному аспекті представляє науковий інтерес твердження О. А. Баранова, який зазначає, що досвід застосування технократичних термінів у правовій науці свідчить про необхідність формулювання дефініцій цих термінів, перш за все, з позицій інтересів права, але з безсумнівним збереженням технологічної (технічної) сутності явища або об’єкта, що описується [2, с. 96].

Ідеєю концепції «Інтернету речей» *(IP або Internet of Things (англ.) або скорочено - IoT)*, яку у 1999 р. сформував британський технолог Кевін Ештон, було впровадження таких механізмів, які б давали можливість речам збирати, опрацьовувати та передавати дані без участі людини. Можливість повної автоматизації передачі даних обговорювалася у науковому світі ще у 1970-х роках, коли з’явився термін «повсюдний комп’ютинг» [3, с. 4]. Трансформація відносин в юридичній сфері, викликана надшвидкими темпами розвитку технічного прогресу, окреслила необхідність наукового визначення та обґрунтування термінологічного апарату. Як вже вище зазначалося, з’ясування природи феномена Інтернету речей, його ролі та значення у соціальному житті для правової науки є вкрай важливим завданням з огляду на необхідність вирішення правових проблем, які пов’язані з впровадженням та використанням у різноманітних сферах діяльності технологій Інтернету речей [1, с. 32].

Дослідження Інтернету речей в комплексному підході до сутності явища дедалі набуває більшого поширення. Із запропонованих визначень, на нашу думку, заслуговує на увагу розуміння Інтернету речей як сукупності взаємодіючих технічних систем і комплексів, призначених для реалізації суспільних відносин, у тому числі, пов’язаних з наданням послуг або проведенням робіт, на основі використання різноманітних даних і мережі Інтернет за безпосередньої участі або без участі суб’єктів цих відносин (юридичних або фізичних осіб) [2, с. 101].

Наукова думка сьогодні стверджує, що IoT не слід розглядати як просту сукупність різноманітних датчиків та приладів, з'єднаних між собою каналами зв'язку та мережею інтернет. Це своєрідний інтеграційний зв'язок двох світів: реального та віртуального, в якому здійснюється взаємодія та спілкування людей і техніки [3, с. 6]. Сфера судочинства є саме тією площиною, де повна автоматизація діяльності є виключеною, завжди має місце поєднання автоматизованих процесів та людської діяльності. Одним із напрямів судової реформи є використання штучного інтелекту для виконання завдань, де людська діяльність є неефективною або ж потенційно небезпечною. Стрімкий розвиток сучасних інформаційних технологій надає широкий спектр можливостей для удосконалення організації органів судоустрою та обмеження впливу «людського фактору» у сферах, де це можливо.

До недавнього часу органи судоустрою, як особливі органи державної влади, які на конституційному рівні наділені повноваженнями здійснювати правосуддя, уособлювала велична постать судді - високоморальної освіченої безсторонньої людини в мантії, за якою залишається останнє слово у вирішенні спору, конфлікту чи встановленні справедливості. Проте, саме через «людський фактор» наразі маємо невтішні статистичні дані, які відображають недовіру судам. За даними соціологічного дослідження Українського центру економічних та політичних досліджень ім. О. Разумкова станом на березень 2021 р. рівень недовіри судам (судовій системі загалом) висловили 79% опитаних респондентів. Водночас сьогодні люди впевнено довіряють Збройним Силам України (довіру висловили 70 % опитаних) та церкві (64% опитаних) [4]. Маємо сміливість зробити припущення, що причина недовіри полягає саме в сумнівах респондентів щодо безсторонності та незаангажованості суддів, а отже це недовіра суддям - людям. Можливості штучного інтелекту забезпечують зменшення впливу людського фактору у тих сферах, де втручання та зловживання є неприпустимими.

Досвід впровадження штучного інтелекту у сферу судочинства є у зарубіжних країнах - Австралії, Китаї, Великій Британії, США. В 2014 в Австралії створили перший «онлайн-суд», тобто функцію суду виконує штучний інтелект. Сьогодні вже функціонують: а) платформа для онлайн-слухань, б) мобільний додаток, який містить перелік «онлайн-судів», в) реєстр електронних повісток, г) електронний реєстр обвинувальних актів, д) електронна система організації колегії присяжних. Всі ці нововведення надають можливість австралійцям на судову процедуру витрачати не кілька годин, а кілька хвилин [5]. У Китаї вперше було створено «онлайн-суд» у 2017 році. У місті Ханчжоу для вирішення спорів у сфері комерції, авторського права, онлайн-послуг застосовується мобільний додаток, на який надсилаються рішення суду. Сьогодні такі суди працюють ще у двох містах - Пекіні

та Гуанчжоу. А ще у дванадцяти китайських провінціях «онлайн-суд» працює на базі одного з месенджерів (WeChat). Існує можливість для учасників справи брати участь у судовому засіданні за допомогою відеозв'язку [5]. Китайський Верховний Народний Суд запровадив систему «подібних рішень для подібних справ» з метою забезпечення ефективного нагляду за діяльністю судів. Система судових рішень для подібних справ передбачає, що критерії вирішення справи узгоджуються між двома складовими: справою, яка зараз розглядається суддею, і подібними справами, які вже розглядалися раніше іншими судами. В Китаї діє «Механізм пошуку обов'язкових подібних випадків та звітності», який впроваджений завдяки великим даним (bid data) та штучному інтелекту: судді мають здійснювати пошук подібних та пов'язаних з ними справ, перш ніж ухвалювати рішення, тим самим забезпечивши узгодженість критеріїв оцінки подібних випадків [6]. У Великій Британії, у зв'язку з тим, що багато документів оформлювалися неналежно, запровадили подання онлайн-заяв. Учасники процесу заповнюють форму, яка містить питання по справі. Цікаво, що раніше 40% заяв про розірвання шлюбу суди були змушені повертати через неналежне оформлення, а завдяки онлайн-формам цей показник знизився до рівня 0,5% [5]. Але головними користувачами штучного інтелекту в системі правосуддя, зокрема в цивільних та кримінальних справах, є Сполучені Штати Америки. Дослідники зі Стенфордського університету розробили алгоритм, який виконує функції асистента судді під час обрання запобіжного заходу підсудному: програма оцінює ризики та дозволяє тримати під вартою значно меншу кількість осіб, зберігаючи при цьому баланс громадської безпеки. Продуктом комерційної компанії «Northpointe» (США) є програмне забезпечення COMPAS (*Correctional Offender Managment Profiling for Alternative Sanctions*), що оцінює ризик повторного скоєння підсудним злочину. Програма COMPAS базується на обробленні даних, отриманих з анкети, заповненої підсудним, а в разі його відмови від такої процедури програма ґрунтується на відомостях з його досьє [7].

Отже, проаналізувавши наукові публікації, присвячені Інтернету речей та штучному інтелекту зокрема, можемо зробити висновок, що питання застосування штучного інтелекту в правосудді залишається актуальним у аспекті розвитку цифрових трансформацій суспільства, а тому потребує подальших наукових досліджень.

Література:

1. Баранов О. А. Інтернет речей (IoT): мета застосування та правові проблеми. *Інформація і право.* 2018. № 2. С. 31-44.

2. Баранов О. А. «Інтернет речей» як юридичний термін». *Юридична Україна.* 2016. № 5-6. С. 96-103.

3. «Інтернет речей»: Бібліографічний покажчик (Споживаємо розумно) / уклад. М. Маслова. Запоріжжя: ЗОУНБ. 2020. 72 с.

4. Довіра до інститутів суспільства та політиків: Оцінка ситуації в країні, довіра до інститутів суспільства та політиків, електоральні орієнтації громадян (березень 2021р.). *Разумков Центр* : веб-сайт. URL: https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-sytuatsii-v-kraini-dovira-do-instytutiv-suspilstva-ta-politykiv-elektoralni-oriientatsii-gromadian-berezen-2021r (дата звернення: 26.04.2021).

5. Електронне правосуддя у різних країнах світу: як все працює. *Судово-юридична газета «СУД ІНФО»*. 7 серпня 2020 р. URL: https://sud.ua/ru/news/sud-info/175875-elektronne-pravosuddya-u-riznikh-krayinakh-svitu-yak-vse-pratsyuye (дата звернення: 26.04.2021).

6. Штучний інтелект в судовій системі: як це відбувається в Китаї. *Future Now: Technologies & Science Blog*.23 квітня 2021 р. URL: https://futurenow.com.ua/shtuchnyj-intelekt-v-sudovij-systemi-yak-tse-vidbuvayetsya-v-kytayi/ (дата звернення: 26.04.2021).

7. Риков В. В. Штучний інтелект на допомогу правосуддю: дотримання прав людини. *Вища школа адвокатури НААУ* : веб-сайт. URL: https://www.hsa.org.ua/blog/shtuchnyj-intelekt-na-dopomogu-pravosuddyu-dotrymannya-prav-lyudyny/ (дата звернення: 26.04.2021).

Студентські виступи

Воронько Марина
Студентка, КПІ ім. Ігоря Сікорського
Науковий керівник: Дубняк М.В.,
к.ю.н., старший викладач
кафедри інформаційного права та
права інтелектуальної власності
КПІ ім. Ігоря Сікорського

ВІДКРИТІ ДАНІ ЯК СКЛАДОВИЙ ЕЛЕМЕНТ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Іще близько 10 років тому цифровізація була чинником обмеження можливості отримання державних послуг чи доступі до правосуддя через недостатній рівень навичок користування технічними пристроями. Проте зараз ситуація змінилась кардинально навпаки: запровадження карантину стимулювало розвиток електронних сервісів взаємодії суспільства з державою та показало цінність оцифрування і розміщення інформації у вільному доступі, що є основною суттю відкритих даних.

Відкриті дані є публічною інформацією у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання [1]. Для України значний розвиток даної сфери почався 2015 року, з запровадження Єдиного державного веб-порталу відкритих даних, хоча історично Україна пропонувала загальнодержавні рішення з залученням систем обробки значної кількості інформації і значно раніше (ідея Віктора Глушкова про запровадження ЗДАС у 1960-х роках). Впровадження і розвиток формату відкритих даних є базовим для реалізації Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки. Головним її завданням визначається інтеграція сервісу data.gov.ua до центрального європейського порталу відкритих даних data.europa.eu [3], що, до речі, за своєю структурою є майже ідентичним до українського. Ідея впровадження відкритих даних була розвинена закордоном, тому Україна намагається коригувати вимоги стандартизації та базових принципів забезпечення доступу до наборів даних відповідно до міжнародного досвіду, а сам реєстр відкритих даних активно

використовує підтримку міжнародних організацій USAID, Фонду Східної Європи та Innovabridge.

«Стратегія цифровізації» ООН вбачає під цифровою активністю два взаємопов'язані процеси - цифровізації та оцифрування. Функціонування формату відкритих даних приймає безпосередню участь у розвитку обох з них.

По-перше, з самого визначення випливає оприлюднення інформації в електронному вигляді за замовчуванням. Саме такий формат дозволяє вільне її використання на широкий загал та легкість доступу: наразі не потрібно писати запит та їхати до розпорядника для ознайомлення з документами, або витрачати кошти і ресурси на ксерокопіювання - це спрощується до декількох «кліків» та займає значно менше часу.

Проте на сьогодні існують значні складності з належністю оприлюднених наборів даних - недодержання формату є найпоширенішим порушенням розпорядників інформації. За п’ятизірковою моделлю оцінки відкритості даних Тіма Бернерс-Лі, яка залежить саме від формату, одна зірка – не обов'язкова вимога машиночитання даних (наприклад, подання у форматі PDF); дві зірки – додається вимога машиночитання даних (наприклад, таких форматів, як XLS і XLSX); три зірки – додається вимога відкритих форматів (наприклад, таким форматом даних є формат CSV); чотири зірки – додається вимога до форматів, щоб вони задовольняли відкритим стандартам RDF; п’ять зірок – присвоюються даним, представленим за моделлю RDF і включеним у світову хмару пов’язаних відкритих даних [5, с. 2]. Навіть у самому Положенні про набори даних, які підлягають оприлюдненню, формати DOC(X), PDF, JPG, PNG визнаються належними [2], що одразу знижує планку якості та зручності використання інформації до найнижчого. Окрім цього, значна кількість наборів даних викладається у форматі, який взагалі неможливо зчитати (у свій час так відбулось, наприклад, з МВС, який опублікував звіти у форматі JSON зі значними помилками) або у вигляді відсканованих документів, використання та обробка яких у певній частині стає неможливою.

По-друге, якість відкритих даних, у процесі застосування цифровізації, впливає на покращення критеріїв ефективності державного управління: зростає рівень прозорості діяльності, зрозумілості, наближення державних процесів до громадян, що дозволяє активніше залучати їх до здійснення народовладдя. Доступ до повної і достатньої інформації підвищує довіру та ускладнює поширення корупції.

Оприлюднення даних у вільний доступ є проміжним, але невід’ємним, етапом до створенні якісних інформаційно-комунікаційних сервісів, надійної систему

документообігу та просторів для консультування представників влади з громадськістю.

По-третє, щоденно для виконання своїх обов’язків державні органи накопичують велику кількість даних. Для розпорядника така інформація може не становити цінності, проте зацікавлені суб’єкту бізнесу чи громадськості зі свого боку можуть запропонувати сотні ідей їх використання: від оптимізації благоустрою біля свого будинку до ґрунтовних змін у механізмах публічного управління, покращення демократії, туризму, економіки, боротьби з корупцією тощо. Аналіз відкритих даних лише набуває своєї популярності, проте має величезний потенціал для покращення життя держави. Так, наприклад, використовуючи відкриті набори даних компанія “Лун Місто” розробляє дослідження якості життя у місті Києві (чистота повітря, трафік, мапа закладів комунальної власності тощо), а на Єдиному державному веб-порталі відкритих даних постійно поповнюється список мобільних додатків, що спрощують життя (моніторинг судових рішень, автоматизація державних реєстрів тощо).

Проте механізм оприлюднення відкритих даних зазнає значних проблем, пов’язаних з безвідповідальністю розпорядників і низькій обізнаності суспільства про цінність інформації. На сьогодні, єдиний веб-портал містить 36 311 наборів даних, що є непоганим результатом, хоча і порівняно невисоким з державами ЄС, Великою Британією або США. Пік активності додавання та перегляду припадає на 2019-2020 роки, проте зараз активність знизилась до рівня 2018 року, що дуже засмучує. Відповідно до статистики, зібраної Державним агентством з питань електронного урядування України, лише 19% розпорядників інформації сумлінно виконують обов’язок щодо оприлюднення відкритих даних, 22% не виконали навіть половини заявлених вимог, а 33% мають 0% звітності [4].

Підбиваючи підсумки хочеться відзначити, що можливою проблемою недодержання законодавства у сфері відкритих даних може бути неефективна юридична відповідальність. Відповідно до чинного законодавства, за неоприлюднення інформації розпорядник несе адміністративну відповідальність у вигляді штрафу від двадцяти п’яти до п’ятдесяти неоподатковуваних мінімумів доходів громадян. Проте доволі несподіваним є те, що реагування на даного виду правопорушення покладено на Секретаріат уповноваженого верховної ради України з прав людини, що викликає питання доцільності таких повноважень, спроможності забезпечити доступність звернення громадян та оперативність реагування. Відповідно до щорічного звіту, за 2020 рік було складено всього 185 протоколів за ч. 1-2 ст. 212-3 (диспозиція якої є значно ширшою ніж неоприлюднення саме

відкритих даних), що викликає сумніви в ефективності застосування встановленої юридичної відповідальності [6, с. 74].

Висновки: Публічна інформація у формі відкритих даних є дуже цінним ресурсом для забезпечення цифрової трансформації суспільства, оскільки вона здатна забезпечити процеси цифровізації та оцифрування. Окрім цього, відкриті дані забезпечують можливість розвитку інституту комунікації громадян та держави, якісно покращують чинники діяльності органів влади та довіри громадян. Аналіз наявних наборів даних становить значний потенціал для створення нового продукту з оптимізації державних та приватних аспектів життя, - тому є вкрай важливим залучення активних громадян, організацій та представників бізнесу до цієї сфери. Проте, на жаль, механізм реалізації доступу до відкритих даних містить значні проблеми з додержанням встановлених вимог, що не дозволяє досягти бажаного рівня результату. Можливим напрямком для покращення ситуації може стати вдосконалення законодавства про юридичну відповідальність за невиконання обов'язку оприлюднення наборів даних розпорядниками інформації.

Література:

1. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Дата оновлення: 24.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 26.04.2021).

2. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних: Постанова Кабінету Міністрів України від 21 жовтня 2015 р. № 835. Дата оновлення: 13.10.2020. URL: https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#Text (дата звернення: 26.04.2021).

3. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. Дата оновлення: 17.09.2020. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (дата звернення: 26.04.2021).

4. Єдиний державний веб-портал відкритих даних: веб-сайт. URL: https://data.gov.ua/ (дата звернення: 26.04.2021).

5. Клімушин П. С, Спасібов Д. В. Інноваційні сервіси відкритих даних для забезпечення ефективного функціонування е-уряду. *Актуальні проблеми державного управління*. 2017. №1(51). С. 1-8.

6. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2020 рік/ *Звіт*. 2021. 355 с.

Полякова Ірина
Студентка, КПІ ім. Ігоря Сікорського
Науковий керівник: Дубняк М.В.,
к.ю.н., старший викладач
кафедри інформаційного права та
права інтелектуальної власності
КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУДОЧИНСТВА І ДІЛОВОДСТВА В СУДАХ УКРАЇНИ

На цей час в українському судочинстві є досить гострою проблема ведення документообігу, що, як наслідок, призводить до порушень як у системі судоустрою взагалі, так і до порушень законних прав та інтересів осіб-учасників справи. У XXI столітті – ері глобальної трансформації суспільних відносин, низка аспектів судочинства є застарілою, а тому потребують значного вдосконалення.

Цифрові технології постійно проникають в усі сфери нашого життя, і правосуддя не виняток. Інформаційна підтримка правосуддя і комп'ютеризація судів – елементи й прояви електронного правосуддя.

Ідея запровадити систему електронного судочинства не є новою для України. Перший фактичний розвиток вона здобула при прийнятті Закону України «Про доступ до судових рішень» [1] від 2005 року, на виконання положень якого було прийнято Указ Президента України «Про Концепцію вдосконалення судівництва для утвердження справедливого суду в Україні відповідно до європейських стандартів» [2].

Сьогодні ключовим елементом електронного судочинства є єдина телекомунікаційна система, однією з підсистем якої є «Електронний суд». Наказом ДСА України від 22 грудня 2018 року № 628 «Про проведення тестування підсистеми «Електронний суд» у місцевих та апеляційних судах» запроваджено тестовий режим експлуатації підсистеми «Електронний суд» у всіх місцевих та апеляційних судах України [3].

На шляху до впровадження Єдиної судової інформаційно-телекомунікаційної системи, яка довгий час чекала на свій запуск, взагалі, та «Електронного суду» зокрема, виникали та виникають різноманітні перепони як об’єктивного, так і суб’єктивного характеру. Цьогоріч, в умовах оголошеного загальнодержавного карантину, Вища рада правосуддя, як орган суддівського врядування, оперативно

здійснила низку кроків та зрушила цю проблему з непохитного місця, щоб частково запустити «Електронний суд» [4, с. 44].

Необхідно зазначити, що впровадження цифрових технологій у судочинство має 2 аспекти:

- інформатизація судів – автоматизація повторюваних рутинних процесів, створення єдиної судової комп’ютерної мережі, автоматизація процесів діловодства та фіксації засідань;
- безпосередньо електронне судочинство – процесуальний засіб здійснення судочинства шляхом проведення відеоконференцій, автоматизація процесу подання заяв та надсилання електронних сповіщень.

Очевидним є той факт, що для повного існування діджиталізованої судової системи необхідна повна реалізація обох аспектів.

Звичайно, під час розвитку процесу віддаленої роботи в суді виник ряд питань, в першу чергу пов'язаних з ідентифікацією фізичних осіб, використанням певного програмного забезпечення державними органами, безпекою і захистом інформації та зберіганням особистих даних. Слід зазначити, що гострою проблемою є непідготовленість інфраструктури суду до віддаленої роботи - не всі суди досі мають відповідне технічне обладнання. Однак у квітні 2020 року українські суди протестували систему відеоконференцзв'язку EasyCon, яка працює з кваліфікованим електронним підписом і дозволяє судам таким чином ідентифікувати людину. Зокрема, за даними судової статистики, показник розгляду місцевими судами кримінальних справ, судове провадження щодо яких здійснювалось в режимі відеоконференції, складає 14% [5].

Надзвичайно важливо, щоб ці технологічні зміни стали реальністю в роботі судів сьогодні, хоча до недавнього часу дещо стало недосяжним. Вважаючи життя і здоров'я людей найвищою соціальною цінністю в умовах пандемії, суди змогли забезпечити і гарантувати право людей на життя і здоров'я, а також право на захист, право на справедливий судовий розгляд. Це безумовний результат. Маємо впевненість в тому, що питання оцифровки правосуддя буде актуальним і після карантину. Останні технології, впроваджені судами під час пандемії, ймовірно, стануть «більш популярними» і більш застосовними, ніж судові процеси в класичному сенсі цього слова.

Слід підкреслити, що Україна, як і увесь світ, стрімко рухається до нового інформаційного суспільства. До суспільства, для якого характерний переклад максимальної кількості дій звичайного людського життя в електронну, інформаційну форму. І судова процедура - одна з таких областей. Деякі кроки в цьому напрямку вже зроблені. І саме епідемія стала так званим «поштовхом» до більш швидкого

прогресу в цьому напрямку, оскільки парламентом було ухвалено «антикоронавірусний закон», норми якого дозволяють сторонам мати більше можливості для участі в судовому процесі в дистанційній формі. Раніше така можливість також була доступна, але учасник процесу повинен був з'явитися в найближчий суд, де мала бути встановлена його особа, і була забезпечена дистанційна участь в розгляді, який проходив у іншому суді. Тепер процедура спростилася. За допомогою різних програм відеоконференцзв'язку у сторін з'являється більше можливостей для проведення розгляду дистанційно, а у судів більше інструментів для ідентифікації сторін.

Звичайно, новітні технології - це, перш за все, нові можливості і оптимізація процесу, але, звичайно, ідея електронного судочинства повинна реалізовуватися одночасно зі створенням правової і матеріальної бази для захисту електронних судових процесів залежить від його неупередженості. Таким чином, незважаючи на кризу, викликану пандемією, вона виявила проблеми з недосконалістю правових норм, технічною неготовністю судів перейти до електронного правосуддя, однак держава рішуче підтримує і розвиває цю сферу.

Зокрема створено Міністерство та Комітет цифрової трансформації, а також у Комітеті Верховної Ради України з питань правової політики створено робочу групу з цифровізації судочинства, де обговорюються питання інновацій для запуску ЄСІТС [4].

Як відзначає заступник голови правління Центру політико-правових реформ Р. Куйбіда, поки що працівники судової системи неохоче використовують можливості електронного судочинства, а ухвал про відмову у задоволенні клопотань щодо розгляду справ дистанційно більше, ніж позитивних вердиктів. Пояснення при цьому даються різні – або недотримання порядку подання чи помилки при оформленні клопотань, або «відсутність технічних можливостей» [6].

Проаналізувавши вищезазначене, можна зробити висновок, що аби запровадити систему електронного судочинства повноцінно, необхідно реалізувати значну кількість завдань, зокрема:

- провести навчання суддів щодо правильного використання та застосування електронного судочинства;
- вдосконалити механізми забезпечення захисту конфіденційної інформації;
- забезпечити суди необхідним обладнанням для можливості користування електронним судочинством.

Наразі в України діє тестовий режим Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС), яка б дозволила перевести судовий процес в повністю дистанційний формат. Впровадження цієї системи у найближчий час все

ще є неможливим, незважаючи на необхідність викликану пандемією. Хоча деякі елементи ЄСІТС, наприклад електронні звернення вже працюють, остаточний її запуск планується лише на 2023 рік [7, с. 28].

Література:

1. Про доступ до судових рішень : Закон від 22 груд. 2005 р. № 3262-IV. Дата оновлення: 24.10.2020. URL: https://zakon.rada.gov.ua/laws/show/3262-15#Text (дата звернення: 22.04.2021).
2. Про Концепцію вдосконалення судівництва для утвердження справедливого суду в Україні відповідно до європейських стандартів : Указ Президента України від 10.05.2016 р. № 361/2006. URL: https://zakon.rada.gov.ua/laws/show/361/2006#Text (дата звернення: 22.04.2021).
3. Про проведення тестування підсистеми "Електронний суд" у місцевих та апеляційних судах : Наказ Державної судової адміністрації України від 22.12.2018 №628. Дата оновлення: 26.04.2019. URL: https://dsa.court.gov.ua/userfiles/media/628_18.pdf (дата звернення: 22.04.2021).
4. Смокович М.І. Електронне судочинство в Україні. *Сучасні виклики та актуальні проблеми судової реформи в Україні* : зб. матеріалів IV Міжнар. наук.-практ. конф., 16 жовт. 2020 р. Київ : Ваіте, 2020. С. 43-47.
5. Судова статистика. URL: https://court.gov.ua/inshe/sudova_statystyka/ (дата звернення: 22.04.2021).
6. Як працює електронне судочинство, або “Встати! Суд на зв’язку”. URL: https://www.ukrinform.ua/rubric-society/3016937-ak-pracue-elektronne-sudocinstvo-abo-vstati-sud-na-zvazku.html (дата звернення: 22.04.2021).
7. Концепція побудови єдиної судової інформаційно-телекомунікаційної системи : Наказ Державної судової адміністрації України від 07.11.2019 № 1096. URL: https://dsa.court.gov.ua/userfiles/media/media/ECITC_Koncepcia.pdf (Дата звернення 22.04.2021)

Sikorinska Alina
student of faculty of biotechnology and biotechnic
Igor Sikorsky Kyiv Polytechnic institute
Supervisor: Olga Golovko,
PhD in Law, Senior Lecturer,
Department of Public Law
Igor Sikorsky Kyiv Polytechnic Institute

EUROPEAN UNION LEGISLATION ON CYBERSECURITY

Network and information systems and electronic communications networks and services play a vital role in society and have become the backbone of economic growth. Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and, in particular, support the functioning of the internal market [4].

Cybersecurity problems arose along with the emergence of information and communication systems (ICS). In this regard, they have been repeatedly considered at various international and national levels, constantly looking for solutions in the context of the development of the ICS themselves [1,3].

First of all, development in the field of combating international and national cybercrime was initiated by the Council of Europe Convention on Cybercrime (Budapest, November 2001). At the same time, it was ratified by more than fifty countries, and among the participating countries were countries that are not members of the Council of Europe, such as the United States, Canada, Japan, Mexico, Australia and many others [2].

The European Parliament, the Council and the European Commission have reached a political agreement on the Cybersecurity Act by creating EU Regulation 2019/881 (Cybersecurity Act), which strengthens the mandate of the EU Cybersecurity Agency (ENISA). The purpose of the law is to support member states in countering cybersecurity threats and attacks. The law also establishes a framework for cybersecurity certification within the EU, enhancing the cybersecurity of online services and consumer devices [4].

The new rules will help people trust the devices they use every day because they can choose between products such as IoT devices that are vulnerable to cybersecurity. The certification system will become a universal cybersecurity

certification center, leading to significant cost savings for businesses, especially SMEs, who would otherwise have to apply for multiple certificates in several countries. Single certification (Article 54 "Elements of European Cyber Security Certification Schemes") will also remove potential barriers to entry. Moreover, companies are interested in investing in cybersecurity of their products and turn it into a competitive advantage [4].

Thus, the process of creating cyber legislation in the EU member states began in 2001 and is still gaining momentum, creating new legislation in this area. The emergence of new technologies and digital information in general leads to the emergence of new legal relations, the settlement of which requires a new approach to the formation of legal norms. An example of successful practices in such a settlement is the EU, in particular in terms of setting up specific cybersecurity bodies and agencies, the most well-known of which is ENISA.

Literature:

1. Vasylenko M. Improving the state of cybersecurity of information and communication systems: quality in the context of improving information legislation. *Legal Bulletin*. 2018. P. 17-24.

2. Vasylenko M. Quality of cybersecurity of information and communication systems (ICS) and some legislative issues regarding its increase. *Legal Bulletin*. 2018. P 13-15.

3. UN General Assembly Resolution “Creating a Global Cyber Security Culture” of December 20, 2002 № 57/239. URL: http://www.un.org/ru/ga/second/57/second_res.shtml.

4. Regulation (EU) 2019/881 of the European parliament and of the council of 17 April 2019 on ENISA (European Union Cybersecurity Agency) and on cybersecurity certification of information and communication technologies and repealing Regulation (EU) №52). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881

Царик Олександра

Студентка, КПІ ім. Ігоря Сікорського
Науковий керівник: Дубняк М.В.,
к.ю.н., старший викладач
кафедри інформаційного права та
права інтелектуальної власності
КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН ПРИ ЗДІЙСНЕННІ КРИПТОВАЛЮТНИХ ОПЕРАЦІЙ

Інтерес до віртуальних (цифрових) грошей у світі постійно зростає. Роль криптовалюти, як засобу: вираження вартості у цифровому форматі; обміну або розрахункової грошової одиниці; зберігання вартості набуває все більшої значимості, при цьому не підпадаючи під поняття легального платіжного засобу. ЇЇ використання в різних сферах життєдіяльності характеризується достатньою зручністю та ефективністю, вона стає певною формою накопичення капіталу. Водночас криптовалюта активно використовуються як у легальній так і нелегальній сферах. Активне використання криптовалюти у протиправній діяльності зумовлює низку загроз та ризиків для стабільного функціонування суспільних відносин, забезпечення національних економічних інтересів. Значні небезпеки виникають з огляду на поширення транснаціональної організованої злочинності, ескалації проявів тероризму у світі.

Процеси світової глобалізації та стрімкий розвиток цифрових технологій зумовлюють виникнення нових загроз національним інтересам нашої держави перш за все в економічній сфері, так як все більшої популярності набувають процеси створення, накопичення криптовалют та проведення операцій з ними. У сучасних умовах зростанню популярності криптовалют в Україні сприяють: їх невизначений правовий статус, анонімність, децентралізованість створення (майнінгу), безконтрольність обігу криптовалют, які нівелюють контрольні функції органів фінансового моніторингу та сприяють їх активному використанню організаціями і групами осіб як у легальній, так і протиправній діяльності.

У даний час на світовому рівні відсутні єдині стандарти регулювання діяльності у сфері створення та обігу криптовалют, їх контролю національними регуляторами. Разом з тим міжнародними установами розроблено і запроваджено низку заходів щодо посилення контролю та моніторингу операцій із

криптовалютами. Директивою ЄС 2015/849 по боротьбі з відмиванням грошей передбачено можливість використання криптовалют та визначено повноваження підрозділів фінансового моніторингу щодо отримання доступу до інформації про криптовалютні гаманці та біржі. [1] Директива ЄС 2018/843, що набула чинності на початку 2020 року внесла зміни у Директиви ЄС 2009/138, 2013/36 і 2015/849 та поширила сферу дії останньої на провайдерів операцій з обміну криптовалют та їх зберігання на електронних гаманцях, надала додаткові повноваження підрозділам фінансового моніторингу з ідентифікації таких операцій. [2] Міжнародна група з протидії відмиванню брудних грошей (FATF) за дорученням лідерів країн G-20 підготувала та оприлюднила 21.06.2019 оновлену Настанову із застосування ризик-орієнтованого підходу до цифрових активів та постачальників цифрових послуг із рекомендаціями для 36 країн-учасниць щодо протидії відмиванню грошей та фінансування тероризму з використанням криптовалют. [3] Зазначені рекомендації спрямовані на недопущення використання криптовалют задля відмивання грошей, фінансування тероризму, а також уникнення існуючих заходів контролю.

06.12.2019 Верховною Радою України (далі ВРУ) було прийнято нову редакцію Закону України «Про запобігання та протидію легалізації (відмиванню) доходів одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», яким передбачено низку ключових положень щодо моніторингу використання віртуальних (цифрових) активів як засобу розрахунку. [4] Однак правовий статус криптовалют, порядок операцій з ними, контролю за їх обігом, функціонування ринку досі залишається неврегульованими.

Варто заначити, що у ВРУ на опрацюванні знаходилось три законопроекти щодо унормування обігу криптовалют в Україні (проекти законів України від 06.10.2017 № 7183 «Про обіг криптовалюти в Україні», від 10.10.2017 № 7183-1 «Про стимулювання ринку криптовалют та їх похідних в Україні», та від 30.10.2017 № 7246 «Про внесення змін до Податкового кодексу (щодо стимулювання ринку криптовалют та їх похідних в Україні). Проте у 2019 році вказані законопроекти були повернуті ініціаторам на доопрацювання. У тому ж році було зареєстровано новий законопроект «Про внесення змін до Податкового кодексу та інших законів України щодо оподаткування операції з криптовалютами». [5] При цьому вказаний законопроект наразі зазнав критики збоку експертного середовища, громадськості та вітчизняного бізнесу.

Сучасні світові тенденції свідчать про активне використання криптовалют у протиправній діяльності, внаслідок чого виникають численні загрози національним

інтересам багатьох країн світу. У грудні 2017 року федеральною прокуратурою США спільно з Об’єднаним Антитерористичним центром Федерального бюро розслідувань було викрито факт використання криптовалюти для відмивання коштів отриманих злочинним шляхом та подальшого фінансування терористичної організації ІДІЛ. [6]

Типові тенденції фіксуються правоохоронними органами Європейського Союзу. Зокрема Європол у дослідженні «Оцінка організованих Інтернет-загроз у 2018 році» [7], що стосується різноманітних проявів онлайн-злочинності, значну увагу надав використанню криптовалют для збору коштів та фінансування онлайн-активності різних терористичних груп.

В Україні, протягом 2016-2018 років невстановленими особами здійснювалося блокування сайтів низки державних установ та ураження їх інформаційних ресурсів шкідливим програмним забезпеченням з вимогами в отриманні винагороди у криптовалюті за їх розблокування.

У 2017 році підрозділами Національної поліції України у ході операції на території м. Києва було припинено діяльність групи осіб, які займалися незаконним майнінгом криптовалют, під час якої вилучено 200 пристроїв для їх генерації. В грудні того ж року викрали одного з керівників криптовалютної біржі «EXMO», що входить до топ-30 світових криптобірж. Викрадачі вимагали 160 біткоїнів, що становить близько 2 млн. доларів США за його звільнення. [8]

Основою для застосування криптовалют є система блокчейн - розподілена мережа, технологія, що дозволяє відкрито та надійно реєструвати інформацію, простежувати шлях транзакцій та зменшувати транзакційні витрати.

Вперше цю технологію було описано у 1991 році Стюартом Хабером та Скоттом Сторнеттою. Однак розвитку блокчейн набула в 2009 році, коли світ познайомився з криптовалютою «біткоїн». Ця технологія себе показала з досить позитивної сторони, що сприяло її подальшому поширенню на світовому економічному рівні, тому зараз ця система використовується не лише в банківській сфері та державному управлінні, а й в повсякденному житті (для цифрового посвідчення особи). [9]

ЇЇ перевагою є те, що децентралізована система готівки не вимагає довіри третім сторонам, процес вилучення чи заміни інформації є неможливим, оскільки вона оновлюються автоматично у разі будь-яких змін та надсилає відповідні дані всім хто має доступ до цієї інформації. Використання даної системи у процесі розрахункових транзакцій підприємцями, допомагає їм зменшити операційні витрати та збільшити обіговий капітал, при цьому, є доказовість кожної транзакції у вигляді криптографічного підтвердження.

В Україні процес становлення технології блокчейн також знаходиться на початковому етапі. Першою спробою закріпити поняття блокчейну на законодавчому рівні була реєстрація 06.10.1017 у ВРУ законопроекту «Про обіг криптовалюти в Україні» [10], де система блокчейн визначається як децентралізованиӥ публічниӥ реєстр усіх проведених криптовалютних транзакцій, які були проведені суб'єктом криптовалютних операцій, а користувачем системи блокчейн є будь-яка фізична особа, фізична особа-підприємець або юридична особа, яка за допомогою власного або орендованого технічного обладнання підтримує працездатність системи блокчейн, здійснює проведення криптовалютних транзакцій та захисту системи блокчейн.

Однак цей крок не дав помітного результату, адже єдиний описаний проект є оглядовим та не охоплює вирішення важливих питань, процесів щодо застосування та впровадження таких технологій, наслідків можливих помилок, тощо.

Перешкодами на шляху впровадження системи блокчейну в Україні є: великі витрати електроенергії, відсутність законодавчої бази та низький рівень адаптації національного законодавства до новітніх реалій у використанні сучасних інформаційних технологій, необхідність досягти консенсусу між великим числом учасників та їх інерцією на ринку.

Об'єктивні ризики, які несе незаконна генерація, обіг та використання криптовалют у протиправній діяльності в Україні вимагають розробку нормативно-правової бази для запровадження чіткого регулювання вказаних процесів, викриття та попередження фактів їх незаконного використання в сфері банківських і небанківських електронних платіжних систем.

Очевидною є необхідність невідкладного вжиття системних заходів на державному рівні в напрямку правового регулювання використання криптовалют та системи блокчейн, удосконалення координації та практичної взаємодії в боротьбі з протиправними проявами в зазначеній сфері, налагодження дієвої співпраці з міжнародними партнерами.

Таким чином, для удосконалення системи правового регулювання у напрямку використання криптовалют та технології блокчейн необхідно запровадити єдину державну стратегію розвитку криптовалютних технологій та правовідносин в Україні; прийняти нормативно-правовий акт, яким визначити правовий статус криптовалют та засади державного контролю і їх обігу; впровадити у практику правозастосування рекомендацій FATF з протидії відмиванню грошей та фінансуванню тероризму з використанням криптовалют, налагодженням належної координаційної роботи відповідних контролюючих і правоохоронних органів з протидії незаконному використанню криптовалют.

Література:

1. Директива ЄС 2015/849 по боротьбі з відмиванням грошей. URL: https://bloomchain.ru/legal/evrope/skij-soyuz-prinyal-novuyu-direktivu-po-borbe-s-kriptovalyutnymi-prestuplenieami/.

2. Директива ЄС 2018/843. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843#.

3. Настанова FATF з ризик-орієнтованого підходу до цифрових активів та постачальників цифрових послуг від 21.06.2019. URL: https://www.fatfgafi.org/publications/fatfrecomendations/documents/public-statement-virtual-assets.html.

4. Закон України про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. URL: https://zakon.rada.gov.ua/laws/show/1702-18#Text

5. Проект Закону України від 15.11.2019 № 2461 «Про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67423

6. Конгресс США изучил отчет об использовании криптовалюты для финансирования терроризма. URL: https://coinzdaily.com/ru/news-ru/bitcoin-ru/конгресс-сша-изучил-отчет-об-использо-8060/.

7. Internet Organized Threat Assessment 2018. URL: www.europol.europa.eu./internet-organized-crime-threat-assessment-2018.

8. Вымогатель PETYA. Что за компьютерный вирус атакует Украину. URL: https://www.ds.news.ua/politics/vymogatel-petya-chto-za-kompyuternyy-virus-atakuet-ukrainu-27062017152500.

9. "Попереду планети всієї": які компанії займаються блокчейном в Україні. URL: https://www.epravda.com.ua/projects/fintech/2019/10/9/652378/

10. Про обіг криптовалюти в Україні : проект Закону України No 7183 від 06.10.2017 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684

Ярош Ілля
Студент, КПІ ім. Ігоря Сікорського
Науковий керівник: Дубняк М.В.,
к.ю.н., старший викладач
кафедри інформаційного права та
права інтелектуальної власності
КПІ ім. Ігоря Сікорського

ІНТЕРНЕТ РЕЧЕЙ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ

Система національної безпеки та оборони потребує належного як правового, так і технологічного забезпечення. Поява технологій здебільшого зумовлена дослідженнями у сфері національної безпеки та оборони. Зокрема, виникнення Інтернету зумовлене саме ними. Проте в подальшому розвиток Інтернету призвів до появи абсолютно непов'язаних з безпекою та обороною процесів та сфер діяльності. Розвиток таких процесів зумовив виникнення Інтернету речей, що був покликаний спростити взаємодію різних технологій між собою, в першу чергу, у побуті, виробництві з метою виконання окремих дій без втручання людини. Однак позитивні практики, пов'язані з Інтернетом речей, стали актуальними і в сфері національної безпеки та оборони. Оскільки подеколи виникають сумніви щодо належного рівня безпеки Інтернету речей, то постало питання доцільності його використання в такій важливій сфері для держави. Саме тому актуально проаналізувати як можливості, що дає Інтернет речей в системі національної безпеки та оборони, так і ризики його використання, а також нормативно-правову базу, покликану його регулювати.

Метою цієї роботи є визначення місця Інтернету речей у системі національної безпеки та оборони.

По-перше, слушно зауважити, що правове регулювання Інтернету речей наразі відсутнє в Україні. Згадки поняття «Інтернет речей» є в Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та плані заходів щодо її реалізації, схваленої розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р [1]. Втім це аж ніяк не регулює Інтернет речей. Водночас в контексті національної безпеки і, разом з цим, безпеки людини дуже важливо, щоб поняття Інтернету речей було висвітлене у нормативно-правових актах, що стосуються, насамперед, кібербезпеки.

Нині чинні нормативно-правові акти, що регулюють питання кібербезпеки, не звертають увагу на Інтернет речей. Водночас спробою окреслити напрямок врегулювання на державному рівні питання Інтернету речей є проєкт Стратегії кібербезпеки України (2021-2025 роки), в якому зазначено, що викликом для України у сфері кібербезпеки є активне використання Інтернету речей [2, с. 7]. Виклик полягає в тому, що «розумні речі» – пристрої, які відносяться до Інтернету речей, поєднані однією глобальною мережею, а рівень захисту від зовнішніх втручань у їхню роботу та кібератак залишається низьким. Як зазначають О. Довгань та А. Тарасюк, головна небезпека Інтернету речей полягає в тому, що ІТ-системи створюють нові точки доступу для зловмисників, які оперують у кіберпросторі – хакерів, кракерів тощо. Так, точкою входу до системи може стати мережевий принтер, який надає хакерам маршрут доступу до комп’ютерів в мережі фінансової організації, або мобільний пристрій, який має доступ до системи радіозв’язку високотехнологічного автомобілю тощо [3, с. 90]. Таким чином, загрози, пов’язані з Інтернетом речей повинні регулюватися на рівні кібербезпеки держави.

Розглядаючи ризики використання Інтернету речей в системі національної безпеки та оборони, можна дійти висновку, що його використання особами, котрі мають відношення до національної безпеки та оборони, доступ до державної таємниці тощо, може призвести до розголошення державної таємниці, негативного впливу на стратегічно важливі рішення або навіть зробити вразливими комп’ютерні системи державних органів, якщо зловмисники знайдуть спосіб підключитися до таких систем через «розумну річ», яка знаходиться поблизу або використовується для спрощення роботи цих систем чи передачі даних на них.

Приміром, у США вищі посадові особи відносять Інтернет речей до глобальних загроз, оскільки такі прилади розроблялися з мінімальними вимогами до безпеки, і тому їх розповсюдженість насамперед у діяльності державних органів та установ становить небезпеку. Таку позицію фактично висловив директор Національної розвідки Дж. Клепер у своїй доповіді в 2016 році [4]. Отже, враховуючи те, що кібербезпека безпосередньо є частиною національної безпеки держави, вважаю, що, з такої позиції, Інтернет речей в системі національної безпеки та оборони є загрозою для її функціонування.

Водночас поряд із ризиками розкриваються можливості, оскільки, на мій погляд, Інтернет речей може стати частиною системи забезпечення національної безпеки та оборони. Відповідно до визначення В. Ліпкана система забезпечення національної безпеки – це комплекс різноманітних заходів (управлінських, нормативних, методологічних, інформаційних, аналітичних, розвідувальних і

контррозвідувальних, пошукових, наукових, технічних, кадрових та ін.), які направлені на оптимізацію процесу управління зовнішніми та внутрішніми загрозами національній безпеці держави [5, с. 57]. Інтернет речей може виступити механізмом, що полегшує інформаційну, розвідувальну діяльність та доповнює технічну складову національної безпеки та оборони.

Дж. Клепер у своїй доповіді в 2016 році прямо зазначив, що у майбутньому спецслужби будуть широко використовувати Інтернет речей для ідентифікації, стеження, спостереження, визначення місця розташування, вербування агентів, отримання доступу до мереж та персональних даних користувачів [4, с. 1]. Звідси слідує, що, попри віднесення Інтернету речей до глобальних загроз, США розглядають його як розширення своїх можливостей в сфері розвідки, контролю за населенням, збиранням стратегічно важливих даних. Хоча, безумовно, інші країни також сподіваються на подібне використання Інтернету речей.

Щодо інформаційної та розвідувальної складової Інтернет речей за своєю суттю є необмеженим джерелом даних, які у разі їх накопичення, комплексної інтеграції та аналізу відповідатимуть основним критеріям розвідувальної інформації та можуть бути безпосередньо чи опосередковано використані національними розвідками для забезпечення інтересів власних держав і підриву позицій країн-супротивників. Також транскордонність Інтернету речей та включення потоку даних в єдину глобальну кібермережу призведуть до зменшення витратної складової, притаманної традиційним видам розвідки [6, с. 110].

Водночас щодо технічної складової Інтернет речей збільшить оборонну спроможність держави. Використання «розумних речей» під час військових операцій, охорони кордону і т.п. дозволить контролювати більшу територію, виявляти потенційні загрози. Так, уже зараз в арміях багатьох країнах світу використовують різні сенсори та пристрої, що здійснюють аналіз пересувань населення, військової техніки супротивника. Хоча ці дії ще вимагають взаємодії людини з технікою, подальша роботизація і розвиток штучного інтелекту усуне цей фактор.

Варто зазначити, що у сфері оборони набувають значення поняття «Інтернет бойових речей» та «військовий Інтернет речей». Фактично, ці поняття описують явище появи в технічному забезпеченні військових підрозділів та армій держав ІТ-технологій. На думку О. Виноградського, літальними або наземними безпілотними апаратами і роботизованими бойовими машинами сьогодні вже важко здивувати. По мірі появи нових технологій спектр завдань і можливостей військових «розумних пристроїв» розширюється швидкими темпами, починаючи від вирішення складних

задач високоточного виявлення і знищення противника, і закінчуючи моніторингом фізичного стану конкретного військовослужбовця [7].

Таким чином, Інтернет речей для розвитку оборонної спроможності держави є невід'ємною складовою. Завдяки ньому будуть змінюватися підходи щодо ведення бойових дій та військових операцій, реагування на конфлікти, системи підготовки військовослужбовців.

Крім того, система національної безпеки потребує швидкої взаємодії між різними відомствами з метою узгодженої та ефективної моделі управління сектором національної безпеки. Враховуючи, що комп'ютерні системи вже давно використовуються для управління та зв'язку, вважаю, що Інтернет речей дає додаткові можливості в цьому напрямку. Зокрема, розширює кількість пристроїв, систем, через які чи за допомогою яких відомства можуть взаємодіяти, віддавати команди, моделювати різні ситуації, що загрожують національній безпеці. Звісно, в цьому випадку спочатку варто подбати про конфіденційність з'єднання таких пристроїв з іншими системами, безпечну передачу даних через них та запобігання можливим несанкціонованим втручанням у їхню роботу, усунути усі проблеми, модернізувати законодавство під сучасні реалії, оскільки питання національної безпеки та оборони є першочерговим у наш час.

Висновки. Місце для Інтернету речей в системі національної безпеки та оборони ще повністю не віднайдене. На мій погляд, переваги Інтернету речей поступово стануть ще помітнішими, а ризики будуть усунуті. З метою усунення ризиків Україні потрібно прийняти низку нормативно-правових актів щодо Інтернету речей. Зокрема, законодавство про кібербезпеку вимагає, як мінімум, згадки та правового визначення поняття «Інтернет речей». Крім того, Кабінет Міністрів України повинен розробити концепцію розвитку Інтернету речей, оцінивши всі його переваги та ризики для національної безпеки та оборони. Це допоможе зробити перші кроки щодо подолання ризиків для системи національної безпеки та оборони, що несе Інтернет речей. Надалі Інтернет речей змінить деякі процеси в системі національної безпеки та оборони: покращиться інформаційна, розвідувальна діяльність державних органів національної безпеки, технічне забезпечення сектору оборони, а також взаємодія між різними відомствами.

Література:

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та плані заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (дата звернення: 20.04.2021).

2. Проєкт Стратегії кібербезпеки України (2021-2025 роки). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 20.04.2021).

3. Довгань О. Д., Тарасюк А. В. Протидія загрозам кібербезпеці держави на глобальному рівні. *Інформація і право.* 2020. № 2 (33). С. 85-98.

4. Clapper J. Worldwide Threats Assessment of the US Intelligence Comminity: Statements for the record. February, 9, 2016. URL: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf (дата звернення: 20.04.2021).

5. Ліпкан В. А. Поняття системи забезпечення національної безпеки України. *Право і Безпека*. 2003. Т. 2. № 4. С. 57-60.

6. Ткачук Н. А. Використання Інтернету речей в розвідувальній діяльності. *Інтернет речей: проблеми правового регулювання та впровадження*: матеріали другої наук.-практ. конф., 29 лист. 2018 р., м. Київ. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. С. 110-113.

7. Виноградський О. Інтернет речей: цивільне і військове застосування. *Defense Express.* 2018. URL: https://old.defence-ua.com/index.php/statti/4250-internet-rechey-tsyvilne-i-viyskove-zastosuvannya (дата звернення: 21.04.2021).

Секції конференції

Абрамович Ірина

студентка КПІ ім. Ігоря Сікорського.
Науковий керівник: Дорогих Сергій,
к. ю. н., старший науковий співробітник
ДНУ «Інститут інформації, безпеки і права
НАПрН України», старший викладач
КПІ ім. Ігоря Сікорського

ШТУЧНИЙ ІНТЕЛЕКТ У КРИМІНАЛЬНО-ПРАВОВОМУ РОЗРІЗІ

Людство протягом тисячоліть мріяло створити штучну істоту, яка мислить і діє по-людськи. І на сьогоднішній день ця мрія нестримно перетворюється в реальність.

Швидкі зміни в нашому суспільстві збільшили кількість технологій, що впливають на наше життя. З кожним роком «машинний розум» починає все більше думати замість нас і полегшувати наше життя, - штучний інтелект (ШІ) перевершив людину у здібності до читання та розуміння тексту (результати людини в відповідному тесті складають 82.304, ШІ компанії Alibaba – 82.440, а Microsoft – 82.650) [1]. Медсестри та хірурги-роботи вже не вигадка. ШІ увірвався вже навіть у процеси, зв'язані з юриспруденцією: юридична фірма Baker & Hostetler оголосила, що вони наймають штучний інтелект «Росс» управляти їх практикою банкрутства, яка складалася з майже 50 юристів [2].

Та як ми знаємо, досі нічого ідеального в світі нема, а Ілон Маск, одна із найбагатших та найвідоміших персоналій сьогодення, взагалі називає ШІ найбільшою загрозою XXI століття.

Звичайно ж можна навести багато прикладів збоїв, які пов’язані з ШІ, хоча вони поки не набули глобального масштабу. Наприклад, «Сбербанк» втрачав мільярди рублів через помилки штучного інтелекту. Про це розповів голова кредитної організації Герман Греф: «Штучний інтелект приймає рішення, як правило, у великих системах. І маленька помилка, яка закрадається в алгоритм, може призводити до дуже великих наслідків », - зазначив Греф [3].

Тому постає питання про те, хто ж в дійсності відповідальний за помилки ШІ?

Якщо брати до уваги різні прогнози, то до 2075 року процеси мислення штучного інтелекту не можна буде відрізнити від мислення самої людини. Уже зараз

технологія ШІ часто використовує методи машинного навчання для обробки великих обсягів даних.

Що ми будемо мати, якщо візьмемо гіпотетичну ситуацію, коли штучний інтелект максимально стане схожий на людський? ШІ вивчає своє завдання поступово, щоб бути ефективнішим та ставати кращим; так само, як і люди - без подальшого програмування. Тобто перша версія самовдосконалюється і так може відбуватись до нескінченності, вирішує завдання за допомогою старих версій самої себе. І в такому випадку нова версія програми ШІ діє уже самостійно від людини і сама «приймає рішення» в тій чи іншій ситуації. Це і стає проблемою у визначенні суб’єкта кримінальної відповідальності, зв’язаної зі збоями механізму штучного інтелекту.

Гонка до створення надрозумної штучної істоти кидає виклик кримінальному законодавству, оскільки контроль людини є одним із важливих ключів при притягненні особи до відповідальності за злочин. Коли ШІ діє автономно, обмежений контроль людини над ШІ здається проблематичним вже.

Загалом теорія кримінального права описує в якості суб'єкта злочину фізичну особу як таку, яка здатна: 1) усвідомлювати фактичну сторону скоєного діяння; 2) усвідомлювати суспільну небезпечність свого діяння та його наслідків; 3) за конкретних умов здійснити вибір між різними варіантами поведінки та здатна керувати своїми діями [4].

Для порівняння, ШІ уже може мати певну здатність усвідомлювати фактичну сторону того, що відбувається, усвідомлювати суспільну небезпечність свого діяння, тільки цей процес здійснюється за допомогою оцінки на кшталт «добре-погане. Також він має можливість за конкретних умов здійснювати певний вибір між тими чи іншими варіантами поведінки та здатність керувати своєю поведінкою (під час проведення операцій, керування безпілотними транспортними засобами).

Як ми бачимо, ШІ має основні ознаки суб'єкта злочину, та все ж ми не можемо прирівняти його то фізичної особи.

У Резолюції 2015/2103 (INL) Європейського парламенту від 16 лютого 2017 року з рекомендаціями Європейської комісії щодо цивільно-правового регулювання робототехніки (далі - Резолюція 2015/2103 (INL)) акцентується на неможливості залучення штучного інтелекту до відповідальності за дії, які спричинили за собою шкоду третім сторонам. Так, згідно з п. "Ad" Резолюції 2015/2103 (INL) відповідальність за заподіяння шкоди може покладатися на одного з так званих агентів (англійської - human agent), а саме: на виробника, оператора, власника або користувача штучного інтелекту. При цьому в процесі встановлення обсягу

відповідальності з боку "агента" одним з головних аспектів визначається факт доведення можливості прогнозування негативних наслідків і запобігання їх [5].

До того ж, Європейський парламент прийняв на розгляд проект резолюції про правовий статус роботів як “електронної особистості (електронної особи)”. Проект Резолюції передбачає наділення роботів статусом “електронної особистості”, яка має специфічні права та обов’язки. Вказана Резолюція має на меті регулювання правового статусу роботів у суспільстві людей. Актуальність цього питання полягає у тому, що дедалі складніше буде визначати особу (сьогодні це поки що розробник або користувач певного об’єкту робототехніки), яка повинна нести відповідальність за дії з боку штучного інтелекту, наприклад, щодо програмного забезпечення з відкритим початковим кодом (коли його розробниками, або тими, хто його вдосконалює, є невизначена кількість осіб), або відносно штучного інтелекту, який сам себе усвідомлює, наділений здатністю до роздумів про себе та оточуючий світ, самонавчання та самовдосконалення, дбає про власне самозбереження та отримання необхідних ресурсів, має здібності до творчої діяльності, приймає самостійні виважені рішення тощо [6].

Тому, ознаками штучного інтелекту як суб’єкта злочину можуть бути наступні: 1) це електронна особа; 2) здатність ШІ усвідомлювати свої дії чи бездіяльність та керувати ними.

Якщо ШІ буде наділений особливим статусом, тим більше стане учасником кримінально-правових відносин, то постає інакша проблема: мета покарання полягає у виправленні засуджених і скоріше за все така кара не зможе бути імплементована до штучного інтелекту. Тому ефективна система вбачається у напрямку компенсаторних економічних важелів за рахунок активів та можливостей самого штучного інтелекту (напр., стягнення на користь держави, компенсація потерпілому) – сплата певної грошової суми у звичайній валюті, транзакція криптовалютою, виконання робіт, надання послуг тощо [7].

Звичайно ж, людство лише стало на шляху до відкриття ШІ чи суперінтелекту, який перевершить людський інтелект. Та ще одне питання залишається відкритим: якщо ШІ вийде за рамки людського розуміння, то чи зможе вона сама контролювати реалізацію заходів відповідальності у випадку правопорушень здійснених штучним розумом, чи можливо виникне нова правова сфера серед самих штучних інтелектів?

Отже, вбачаються підстави до наступних висновків: перенесення значного сектору життєдіяльності людини до віртуальних світів є неминучою подією, а штучний інтелект (електронна особа, особистість) може бути наділений здатністю усвідомлювати фактичну сторону, усвідомлювати суспільну небезпечність своєї дії або бездіяльності та їх наслідків, керувати своєю поведінкою і може бути визнаний

суб’єктом злочину; але такі зміни можливі лише за умови повного переосмислення системи кримінального права.

Література:

1. Fenner Robert. Alibaba's AI Outguns Humans in Reading Test / Bloomberg Technology, 15 Jan 2018. – Mode of access : https://www.bloomberg.com/technology.

2. Сімсон О. Для захисту креативних ідей авторського права недостатньо [Електронний ресурс] / Ольга Сімсон. – 2019. – Режим доступу до ресурсу: https://creativity.ua/business-and-innovations/olga-simson-dlja-zahistu-kreativnih-idej-avtorskogo-prava-nedostatno/.

3. Сбои искусственного интеллекта [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://newdaynews.ru/technology/656354.html.

4. Бажанов М.І. Кримінальне право України : підручник / М.І. Бажанов. – К. : Юрінком Інтер, 2005. – Режим доступу : http://www.ebk.net.ua/Book/KPravo/10-15/10145.htm.

5. Кто несет ответственность за ошибки искусственного интеллекта? [Електронний ресурс] – Режим доступу до ресурсу: https://uz.ligazakon.ua/magazine_article/EA012676.

6. Радутний О.Е. Кримінальна відповідальність юридичної особи стане кроком до закріплення віртуальності життєвого простору // Електронне наукове фахове видання Національного університету “Юридична Академія України ім. Ярослава Мудрого”. – № 1/2011. – Режим доступу : http://nauka.jur-academy.kharkov.ua.

7. Радутний О.Е. Стан інформаційно-законодавчої діяльності на прикладі Кримінального кодексу України // Інформація і право. – № 3(18)/2016.

Балінська Валерія

Студентка, КПІ ім. Ігоря Сікорського

СТАН ВПРОВАДЖЕННЯ В МІСТАХ УКРАЇНИ ЕЛЕМЕНТІВ ТА МЕХАНІЗМІВ «РОЗУМНОГО МІСТА»

Щоденно звичні для нас речі із неймовірною швидкістю перетворюються у щось нове та більш зручне, підлаштовуючись під сучасні реалії та відповідаючи людським можливостям. Лише 10-15 років тому ми із захопленням дивились на загадкові інтерактивні міста із розумними будинками у фантастичних фільмах, а вже зараз людство активно починає реалізовувати вигадки на практиці. Відтак, виникла необхідність в окресленні такого поняття, як «інтернет речей».

Науковці у галузі інформаційного права у своїх наукових роботах пропонують власні визначення даного поняття. Так, Баранов О.А. під поняттям інтернету речей розуміє сукупність взаємодіючих технічних систем і комплексів, призначених для реалізації суспільних відносин, у тому числі, пов’язаних з наданням послуг або проведенням робіт, на основі використання різноманітних даних і мережі Інтернет за безпосередньої участі або без участі суб’єктів цих відносин (юридичних або фізичних осіб)[1].

У той же час, Бондарев О. визначає інтернет речей як глобальну мережу підключених до Інтернету фізичних пристроїв – «речей», оснащених сенсорами, датчиками і пристроями передачі інформації, що об'єднані за допомогою підключення до центрів контролю, управління і обробки інформації[2].

Однак, основною проблемою у сфері використання технологій інтернету речей є відсутність законодавчо закріпленого поняття у нормативно-правових актах України. Відтак, відсутність належного правового регулювання може спричинити виникнення прогалин на практиці у разі виникнення спорів, пов’язаних із впровадженням елементів «інтернету речей» у повсякденне життя людини.

Одним із наймасштабніших прикладів застосування Інтернету речей є введення його ключових елементів у побут людини та її навколишнє середовище, а відтак створення системи «розумних міст». Першим прикладом такого міста (Smart City) було курортне місто Сантандер (Іспанія), де за допомогою 16 тисяч датчиків по всьому місту можна було отримати інформацію про забрудненість повітря, інтенсивність руху транспорту, вільні місця на парковках, заповнення сміттєвих контейнерів. Одержану інформацію представники влади використали для економії

вуличного освітлення, поліпшення збору відходів і розвантаження доріг. Відтак, основна мета впровадження даних систем була направлена на збір і аналіз інформації, пов’язаної із екологічною ситуацією в населеному місці.

На сьогоднішній день у світі вже створено понад тисячу «розумних міст», які знаходяться в Китаї, Європі, Японії та Північній Америці.

Слід розібратись, які елементи «розумного міста» наразі приносять найбільше користі і які з них вже було впроваджено в українських містах:

- Розробка системи датчиків, що допомагали б збирати інформацію про стан навколишнього середовища (рівень забрудненості повітря, води) та передавати її одразу спеціальним установам з метою подальшого покращення екологічної ситуації в місті. Дані технології вже були впроваджені в таких країнах як Іспанія, Нідерланди, Китай. З червня 2019 року на вулицях Києва за сприяння владних структур також були встановлені системи, що допомагають отримувати інформацію про стан повітря, а також освітленість даної території, що допомагає контролювати належний екологічний стан в столиці.
- Створення «розумного транспорту», що допомагає аналізувати загальну ситуацію на дорогах, має JPS-датчики, що дозволяють людям відстежити їх місцезнаходження, а також оснащені пристроями для сплати за проїзд карткою. На сьогоднішній день дані технології впроваджені у більшості міст Європи, а також у Львові, Києві та Тернополі.
- Розробка мережі відеоспостережень на вулиці, що допомогла б працівникам правоохоронних органів слідкувати за станом злочинності та в окремих випадках – встановити особу злочинця, отримавши належний відео доказ.

Ще у 2017 році рішенням Київської міської ради було затверджено Концепцію «Київ смарт сіті 2020», що включала три ключові рівні змін:

- технологічні – створення сучасної ефективної платформи управління міською інфраструктурою;
- зміни в управлінні містом – зростання прозорості адміністрування та управління містом, розроблення прозорої та конструктивної моделі державно-приватного партнерства;
- суспільні зміни – розвиток сучасної соціальної інфраструктури та рух до соціальної рівності [3].

На сьогоднішній день ми маємо змогу проаналізувати рівень реалізації даної Концепції на практиці. Зокрема, у сфері безпеки дорожнього руху запущено систему відеоспостереження, яка дозволяє розпізнавати обличчя і номерні знаки авто, що дозволяє зменшити час пошуку правопорушників. У той же час, проїзд у муніципальному транспорті столиці запрацював за електронним квитком, який дає

можливість не лише заощадити кошти на кожній поїздці, а й зекономити час на його придбання.

Важливим кроком на шляху використання можливостей «інтернету речей» стало надання доступу пасажирам метрополітену до 4G інтернету, що дозволяє бути на зв’язку навіть під час вашої поїздки.

Також, представниками IT-сфери було розроблено та введено в дію мобільний додаток «Kyiv Smart City», що значно спростив життя киян, завдяки таким сервісам як оплата проїзду за допомогою електронного квитка, сплата штрафу за порушення правил паркування, оплата комунальних послуг та можливість голосування за проекти Громадського бюджету[4].

Якими б зручними та якісними не були такі масштабні оновлення, варто звернути увагу й на ті загрози, які виникли у зв’язку з впровадженням даних технологій.

Хоч дані елементи «розумного міста» і не надають доступу до особистих сторінок та пошти громадян, ризик викрадення інформації, отриманої за допомогою даних систем, а також ймовірність кібератак, з метою виведення систем з ладу, лишаються одними з найактуальніших питань сьогодення. Відтак, виникає необхідність у модернізації законодавства в контексті врегулювання понять інтернету речей, розумного міста та їх структурних елементів, а також важливо розробити належну систему захисту з метою уникнення ситуацій виведення систем із ладу.

По-друге, важливим є питання приватності та конфіденційності життя особи у зв’язку з розміщенням відеокамер на вулицях міста. З одного боку, дані можливості дійсно сприяють зменшенню показника рівня злочинності, а з іншого – певним чином посягають на конституційні права особи. Відтак, виникає необхідність окреслення на законодавчому рівні кола осіб, яким надано право на доступ до зібраної інформації.

Висновки: В процесі дослідження «інтернету речей» та створення з його допомогою «розумних міст» можна дійти висновку про високий рівень людських можливостей та бажання людини зробити своє життя комфортнішим та легшим. Однак, в погоні за мрією, варто пам’ятати про можливі загрози, що можуть нависнути над цілим людством через створення окремих механічних систем. Відтак, саме з метою мінімізації можливих негативних наслідків, існує нагальна необхідність в розробці системи законодавства, що відповідала б сучасним реаліям і належним чином врегульовувала усі існуючі зараз проблемні моменти.

Література:

1. Баранов О.А. «Інтернет речей» як правовий термін / О.А. Баранов // Юридична Україна. – 2016. – № 5-6. – с. 96-103.

2. Бондарев О. Лекторій. Що таке інтернет речей і навіщо він потрібен? URL: http://nv.ua/ukr/science/lectures/lektorijshcho-take-internet-rechej-i-navishcho-vin-potriben-1326653.html

3. Концепція «Київ смарт сіті 2020», затверджена рішенням Київської міської ради від 2017 року. URL: https://issuu.com/kyivsmartcity/docs/kyiv-smart-city-concept

4. Інтерв'ю Юрія Назарова від 28.12.2020 року. URL: https://delo.ua/econonomyandpoliticsinukraine/jurij-nazarov-u-2021-roci-poslugami-rozumnogo-m-376835/

Березіна Катерина

Студентка, КПІ ім. Ігоря Сікорського,

ПОРІВНЯЛЬНО-ПРАВОВІ ДОСЛІДЖЕННЯ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА ТА ЗАКОНОДАВСТВА ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Проблема низького рівня правової обізнаності громадян, пов'язана із захистом власних персональних даних. Пересічна людина яка стає учасником інформаційних відносин, даючи різного роду згоду, нерідко вимушена ставити себе у нерівні права, у порівнянні з іншою стороною. Досить часто люди, які дають згоду в Інтернеті на обробку персональних даних, навіть не уявляють, ким і задля чого їх персональні дані будуть використані.

За для захисту персональних даних необхідно дослідити та порівняти національне законодавство, а саме Закон України «Про захист персональних даних» та Регламент Європейського Парламенту і Ради про захист фізичних осіб при обробці персональних даних (далі – Регламент).

Критеріями даного порівняльно-правового дослідження слугуватиме принципи обробки персональних даних.

Відповідно до ст. 2 Закону України «Про захист персональних даних» персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [2].

Дані принципи є фундаментальними засадами правового регулювання у сфері персональних даних.

Ключові принципи обробки персональних даних:

1. законність обробки;
2. конкретизація мети;
3. відкритість і прозорість обробки;
4. якість даних.

Законність обробки персональних даних

Відповідно до національного законодавства обробка персональних даних має здійснюватися для конкретних і законних цілей, визначених за згодою суб’єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством [2].

Відповідно до Регламенту обробка персональних даних вважається законною якщо дотримано нижченаведені умови:

1. суб'єкт даних надав згоду на опрацювання своїх персональних даних;
2. опрацювання є необхідним для виконання контракту, стороною якого є суб'єкт даних, або для вжиття дій на запит суб'єкта даних до укладення договору;
3. опрацювання є необхідним для дотримання встановленого законом зобов'язання, яке поширюється на контролера;
4. опрацювання є необхідним для того, щоб захистити життєво важливі інтереси суб'єкта даних або іншої фізичної особи;
5. опрацювання є необхідним для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера;
6. опрацювання є необхідним для цілей законних інтересів контролера або третьої сторони, окрім випадків, коли над такими інтересами переважають інтереси фундаментальних прав і свобод суб'єкта даних, що вимагають охорони персональних даних, особливо, якщо суб'єктом даних є дитина [1].

Отже, можемо відзначити що в Регламенті наведено ширше значення принципу законності обробки персональних, тому що зазначено чіткі критерії – виключний перелік умов, в яких обробка персональних даних визнається можливою.

Конкретизація мети обробки персональних даних

Відповідно до ст. 6 ЗУ «Про захист персональних даних» мета обробки має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних [2].

Регламент визначає, що персональні дані необхідно збирати для визначених, чітких і законних цілей і в подальшому не опрацьовувати у спосіб, що є несумісним з такими цілями; подальше опрацювання для досягнення цілей суспільних інтересів,

цілей чи цілей наукового чи історичного дослідження або статистичних цілей не можна вважати, несумісним з первинними цілями [1].

Отже, мета обробки персональних даних повинна бути чіткою і законною, а також визначеною до початку їх збору.

Чіткість формулювання мети має забезпечувати встановлення базових меж обробки персональних даних, що, по-перше, надаватиме суб'єкту персональних даних уявлення про те, якого результату прагне досягти володілець, та, по-друге, не даватиме володільцю невизначених можливостей щодо обробки персональних даних.

Метою обробки персональних даних не може бути сама обробка. Тому мета не може бути сформульована так, наприклад як «необхідність ведення обліку», «накопичення якомога більшої кількості інформації» тощо.

Відкритість і прозорість обробки персональних даних

Даний принцип гарантує особам можливості знати як і ким обробляються, використовуються їхні персональні дані.

Як зазначено в національному законодавстві обробка персональних даних повинна здійснюватися відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки [2].

Обробка персональних даних не може бути прихованою від суб'єкта персональних даних, суб'єкти персональних даних мають право на доступ до своїх даних, де б вони не оброблювалися, якщо інше не встановлено законом. Тож законом можуть передбачатися винятки з цього правила, якщо демократичне суспільство їх припускає, зокрема у випадку здійснення негласних слідчих (розшукових) дій.

Задля забезпечення принципу прозорості володілець персональних даних повинен повідомляти суб'єкта персональних даних про склад і зміст зібраних персональних даних, його права, визначені законом, мету збору персональних даних та третіх осіб, яким передаються його персональні дані. Повідомлення має відбуватися в порядку встановленому законодавством.

Якість даних

Під якістю даних розуміється низка обов'язкових вимог до персональних даних що обробляються, дотримання яких володілець має забезпечити в процесі здійснення всіх операцій з обробки персональних даних.

Якщо обробка персональних даних здійснюється з метою виконання повноважень державного органу, то оброблятися повинні лише ті персональні дані, які необхідні для належного виконання цих повноважень. З огляду на те, що в таких випадках обробка здійснюється тільки на підставах та в порядку, визначених

законом, то саме нормативно-правовими актами повинні визначатися і якісні характеристики даних, які оброблятимуться.

Комплексний аналіз принципів обробки персональних даних в ЄС в цілому свідчить про сформованість правового інституту захисту персональних даних в ЄС, що в свою чергу безпосередньо позитивно впливає на формування даного інституту і в Україні.

Проте, роль технологічного прогресу та процесу глобалізації, розвиток інформаційних технологій, методів автоматизованої обробки даних, формування глобальних інформаційних систем гостро ставить перед європейською спільнотою та Україною особливо питання постійного удосконалення правового та технічного регулювання захисту персональних даних. Перспективи подальших досліджень, пов’язані із необхідністю вивчення нових тенденцій розвитку інституту захисту персональних даних в ЄС на основі триваючих на сьогодні правових реформ у цій сфері та пошуком можливостей впровадження найкращого європейського досвіду в законодавство України.

Література:

1. Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних: Директива 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 24.04.2021).

2. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 24.04.2021).

3. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. 216 с.

Belousova Katerina

1st year student of the Faculty of Sociology and Law The National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»

Supervisor: Inna BORKOVSKA,

Associate Professor, The National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»

LEGAL RESPONSIBILITY IN THE INFORMATION FIELD

It should be noted that there is no unique definition of "legal responsibility" and different scholars interpret it differently. I. Samoshchenko defines legal liability as state coercion to comply with the requirements of the law, reaction to the offense [1, p. 6-11]. S. Alekseev determines that legal responsibility lies in the obligation of a person to transfer measures of state coercive influence for the committed offense [2, p. 48]. M. Strohovych writes that legal responsibility is, first of all, the responsible attitude of the person to the duties, responsibility for correct performance by the person (physical and legal - the citizen and the official, the public organization and the state body) of the duties imposed on it by law [3, p. 73].

Legal responsibility also applies to information law. This is due to the scientific and technological revolution and the transition of society to a qualitatively new state – information. What does information offense mean? It is a socially dangerous, illegal act (or inaction) of a person capable of committing a crime, committed in the information sphere and (or) using information tools and technologies to work with information, regardless of its form, or in other areas of human activity in the information environment [4, p. 207]. The structure of the offense includes four mandatory elements (features): the object, the objective side, the subject and the subjective side.

As for the object, there is documented or publicly announced information about events and phenomena in the field of politics, economics, culture, health care, as well as in social, environmental, international and other. As for the subject, it can be individuals and legal entities depending on the type of legal liability.

Violation of the legislation of Ukraine on information entails disciplinary, civil, administrative or criminal liability in accordance with the laws of Ukraine. For example, The Code of Ukraine on Administrative Offenses provides for administrative liability for

violation of the right to certain types of information, refusal to provide information, providing incomplete or inaccurate information, loss of information. Such offenses include Article 188-19 of the Code of Administrative Offenses "Violation of legislation in the field of personal data protection"; Article 212-2 of the Code of Administrative Offenses "Violation of the legislation on state secrets"; Article 212-3 of the Code of Administrative Offenses "Violation of the right to information and the right to appeal" and other norms [5]. The issue of administrative liability of legal entities for committing offenses in the information sphere needs special attention. The analysis of the norms of the Code of Administrative Offenses shows that only natural persons can be the subject of an administrative offense. However, the current legislation contains cases when legal entities are brought to legal responsibility, in particular in accordance with Part 3 of Article 18 of the Law of Ukraine “On Printed Mass Media (Press) in Ukraine” the court terminates the publication in case of dissemination of information prohibited. Article 46 of the Law of Ukraine "On Information", calls for the seizure of power, forcible change of the constitutional order or territorial integrity of Ukraine; propaganda of war, violence and cruelty; incitement to racial, national, religious hatred; terrorist acts and other criminal acts [6].

Technical progress in the information sphere is happening rapidly. These processes have put the legislator in front of the need for effective legal regulation of public relations in the information sphere. In line with this trend, a number of new regulations have been adopted in the field of information over the last decade.

However, there are gaps in the legislation that address important issues of preservation and protection of information and use of the Internet. Unresolved legal issues contribute to the abuse of information freedom and uncontrolled harmful activities in the information sphere, including the use of information technology. The use of information technology significantly accelerates information processes, but complicates the legal regulation of this issue and leads to increased social tensions.

In order for the legislator to be able to respond quickly and correctly to negative trends in the field of technical progress, legal science should carefully analyze, look for new remedies, as well as develop scientific and practical regulations to address such gaps in legislation.

Legal regulation of the information sphere is in a state of formation due to what has appeared relatively recently. Currently, there is no concept of "information responsibility" in national legislation, but legal responsibility in the field of information offenses exists and needs further study and analysis.

References:

1. Samoshchenko, I. S. (1971) *Responsibility under Soviet legislation*. Moscow [in Russian].

2. Alekseev, S. S. (1972) *Problems of the theory of law: a course of lectures*. Sverdlovsk [in Russian].

3. Strogovich, M.S. (1979) *The essence of legal responsibility*, p. 72-78. Kyiv [in Ukrainian].

4. Polushkin, A. V. (2009) *Signs of information violations*, p. 53–56. Moscow [in Ukrainian].

5. Code of Ukraine on Administrative Offenses. (1984). *Vidomosti Verkhovnoi Rady Ukrainy*. Kyiv: Parlam. vyd-vo [in Ukrainian].

6. Law of Ukraine of printed mass media (press) in Ukraine №2782-XI (1992, November 16) *Vidomosti Verkhovnoi Rady Ukrainy.* Kyiv: Parlam. vyd-vo [in Ukrainian].

Butok Alexandra

student of Faculty of Linguistics,
Igor Sikorsky Kyiv Polytechnic Institute
Supervisor: Olga Golovko,
PhD in Law, Senior Lecturer,
Department of Public Law
Igor Sikorsky Kyiv Polytechnic Institute

CYBER-SECURITY IN TERMS OF TRANSLATION (BASED ON THE WEBSITES AND DOCUMENTS OF THE EUROPEAN UNION)

The importance of cybersecurity policy for the European Union websites is difficult to overestimate. Since the problem of cyber protection covers a variety of vital aspects, the European Union has already issued a series of documents with the view of indicating its legal position toward the cybersecurity measures. These include the European Guidelines and Principles for Internet Resilience document and the Cyber Security Strategy [1]. Nowadays by virtue of extremely quick development of IT, the issue of cybersecurity provision is one of the most essential tasks for the community on the whole.

Cybersecurity is defined as an aggregate of preventive and reactive actions, taken in order to protect the users from threats to their confidentiality in the cyberspace, to provide

safety of Web usage. This notwithstanding, the cyberspace of the organisation is constantly being enriched with brand-new programmes and technologies, every single of which possess principles of compliance with the norms of cybersecurity. Owing to a lack of investigation in the area of the recently developed EU translation tool, the topicality of this research is high.

Term ‘eTranslation’ means a multilingual online translation tool established by the European Commission, which serves for a translation support with the help of IT in all countries-members of the EU [2]. It is bound with such systems as the European Employment and Social Security Information System (EESSI), the Internal Market Information system (IMI), the Online Dispute Resolution system (ODR) etc. Taking into consideration that more than fifty other EU services are already connected with the lately established programme, it only highlights the necessity of conducting a potent cybersecurity policy.

The most essential feature of the product to discuss is its high security. All data translated with the help of the tool is constrained within the cyberspace of the EU and cannot escape it. Thus, the translations cannot be obtained by the outsiders. As it performs translation from and into all 24 official languages of the EU, the materials are available to the citizens of all EU member countries.

The first key point of the cybersecurity policy of the service is a restricted access. Directly the system can be accessed by the staff employed on the positions of EU institutions only. For this a special EU login and credentials are used. Other workers of administration and enterprises have to be registered. It is worth mentioning that the language faculties of universities in the EU are also allowed to use the tool after registration. In case of a yearly non-usage, the individual profile is automatically deleted by the system with the view of preventing cyberpollution [1].

The second reference to compliance with the cybersecurity norms is a privacy statement. Registration means a person approves of their personal information being used by the ‘eTranslation’. The programme notes the access to the system, precise time of log-in, source and target languages, the size of a submitted file. Finally, it registers an e-mail domain so that the user’s requests could be processed. For reasons related to safety, it also automatically scans the content of a submitted document. The files are preserved for a year and a half and then archived. Data is guaranteed not to be shared with third parties [1]. The grounds for usage of personal information by the system are absolutely law-based. Firstly, it is employed to deliver the translated document to the user or to the individual workspace. Secondly, it helps the representatives of administration to resolve technical faults, malfunctions of the programme or even mistakes in translations,

discovered by users. Thirdly, it is required for the production of the usage frequency of the service, with all statistics anonymised.

Another point worth considering is an assurance of personal data minimization. It includes employing pseudonyms, for instance. The complete email address is taken for performing a necessary request once the user logs in the service. As soon as the translated file has been emailed, the information is erased. The required personal data usually includes a EU login, username, name, surname and an email addressed domain. However, for machine-to-machine access through the in EU tools personal information is not required. With the view of cyber legality, the data retrieved from any user is not reserved in the archives. It can also be immediately deleted upon request of a user. Moreover, it can be accessed solely by the managers of the service. These also have a right to process the translations performed by the system in order to avoid any cyberattacks [2].

Consideration of the rights of users, who present their personal information plays a pivotal role in complying with the basics of cyber security. According to the General Data Protection Regulation [3], the eTranslation is obliged to preserve such rights as follows: a right of access by the data subject (article 15); a right to rectification (article 16); a right to erasure (article 17); a right to restriction of processing (article 18); a notification obligation regarding rectification or erasure of personal data or restriction of processing (article 19); a right to data portability (article 20); a right to object (article 21); rights related to automated individual decision making, including profiling (article 22) [4].

The policy on protection of users regarding to the retrieval of any personal information is ensured by the regulations of EU bodies, institutions and offices. It concerns all EC sites and services. The notifications about the use of personal data are sent in separate statement on privacy policy. With the respect of cyber security policy, managers guarantee the conformity with the laws. In a statement on privacy policy the ‘eTranslation’ management provides the specification of collected data, the purpose of retrieval, the technical means, the regulations on accessing it, the term of keeping the retrieved information, the means of safeguarding personal information, the contacts and FAQ section. Users have the right to verify, modify or delete personal information.

As additional measures related to cybersecurity, the service conducts cookies policy. In case accepted, cookies will be enabled to store the language of users, their preferences. They can also store information as to any potentially dangerous or politically sensitive documents submitted for translation. Moreover, cookies help to define whether users have participated in surveys in order not to ask again.

All things considered, the cyberspace of the European Union is heavily protected, as cybersecurity is considered to be one of the top priorities there. Among the latest

innovations of the European Commission is an ‘eTranslation’ tool. Not only is it one of the best CAT-services, but also a sample of compliance with the cyber protection norms.

References:

1. Personal Data Protection Policy. (2018, March 25). Retrieved from https://ec.europa.eu/info/privacy-policy_en#personal-data-protection.

2. Machine translation for public administrations – eTranslation. (2017, November 15). Retrieved from https://ec.europa.eu/info/resources-partners/machine-translation-public-administrations-etranslation_en.

3. General Data Protection Regulation. (2018, May 23). Retrieved from https://gdpr-info.eu.

4. Register of Data Protection Officer (DPO). (2020, January 22). Retrieved from https://ec.europa.eu/dpo-register/detail/DPR-EC-00600.1.

Bukhanets Viktoriia

Student of Faculty of Biotechnology and Biotechnics
Igor Sikorsky Kyiv Polytechnic Institute
Supervisor: Olga Golovko,
PhD in Law, Senior Lecturer,
Department of Public Law
Igor Sikorsky Kyiv Polytechnic Institute

PROSPECTS FOR THE IMPLEMENTATION OF STATE POLICY IN THE FIELD OF ARTIFICIAL INTELLIGENCE IN ACCORDANCE WITH EU POLICY

Modern progress in the field of information technology significantly expands our capabilities, in particular, artificial intelligence (AI) technology helps to solve a variety of problems in the social, scientific, economic spheres, thus making our lives more convenient and comfortable. At the same time, the use of such technologies does not allow to successfully solve the full range of problems, and there are problems of safety and responsibility that require careful study. Therefore, there is a need to develop and implement a regulatory framework that would provide the necessary level of regulation for all issues related to the use of AI that currently exist. To this end, on December 2,

2020, the Cabinet of Ministers of Ukraine approved the Concept for the Development of Artificial Intelligence in Ukraine. However, the question of how the Concept corresponds to the modern vision of the European Union to solve the problem of regulating the use of AI remains open.

The approved Concept defines the purpose, principles and objectives of the development of artificial intelligence technologies in Ukraine as one of the priority areas in the field of scientific and technological research. One of the main problems to solve the need to develop a unified coordinated state policy is the low level of digital literacy and awareness of the population, the low level of investment in the development of AI technologies, their implementation and enforcement. It is also the imperfection of the legal regulation of AI and legislation on personal data protection. Significant problems are the insufficient level of quality of secondary and higher education, lack of funding for research in the field of AI, as well as insufficient information security and data protection in national information and telecommunications systems, increasing number of unauthorized attempts to interfere with automated systems, etc. [1].

Through the implementation of this Concept, the state plans to build a competitive national economy, improve the system of public administration, justice, satisfy the rights and interests of ordinary citizens and business entities, and directly public authorities. Priority areas in which the tasks of state policy of AI development are implemented include education and vocational training, science, information security, cybersecurity, defence, economics, public administration, justice, legal regulation and ethics [1].

Of course, this Concept finds an effective and constructive solution to all problems related to the implementation of artificial intelligence technologies in various spheres of state activity. At the same time, the provisions of the Concept do not sufficiently address the quality and safety of digital products and services, in particular the liability of manufacturers and the risks posed by the use of AI technologies. This may create distrust in these technologies by industry and consumers, which will negatively affect the process of implementing AI technologies in Ukraine. Therefore, in order to ensure the protection of both the consumer and the manufacturer, it is necessary to introduce regulatory regulation of safety and liability.

According to the European Commission document "Report on the consequences for the safety and responsibility of artificial intelligence, the Internet of Things and robotics" from 19.02.2020, several types of risks can be identified when using AI technologies. First, there are gaps in the security of a product or production software that can be used for malicious purposes. Second, there is the risk of losing the device's connection, which can also pose a threat to user safety (such as driving control by AI). The possibility of making AI systems through self-learning, unexpected or unplanned decisions can also be

considered a risk, which raises the question of the need for human control over this process and the management of appropriate settings. Also, the future "behaviour" of AI programs may pose a risk to the mental health of users. It is essential to take into account the receipt of accurate and up-to-date data by AI systems and to introduce specific requirements for mechanisms to maintain data quality throughout the use of AI products and systems. It is necessary to establish requirements for the transparency of AI algorithms, as well as for reliability and accountability. Risks arising from the complexity of products and systems, their impact on each other's functioning can also affect safety [2, p. 5-9]. Thus, it is necessary to develop concepts that take into account the various mechanical, chemical, electrical, cyber risks when using AI systems, and provide possible effective means to reduce these risks.

The use of new digital AI technologies requires a revision of the legal framework regarding the liability of manufacturers for damage caused by their products with AI systems. It is necessary to assess whether the challenges of new technologies to existing structures can lead to legal uncertainty as to how existing laws will be applied, in particular how the notion of guilt will be applied to self-inflicted AI or what can be considered the AI's fault. It is important that companies are aware of their risks of liability throughout the value chain, as well as be able to reduce or prevent them and effectively insure against these risks. Appropriate compensation for damage caused by products that are defective through software or other digital functions should be considered when developing appropriate provisions and concepts. It is also necessary to take into account the fact that different digital devices and services that use AI are combined into a complex system, their interaction with different entities and traditional technologies. After all, this will complicate the assessment of potential damage and finding a responsible person. It is necessary to establish the limits of liability of the manufacturer in the production of products with AI technology and after the introduction of goods into circulation. This includes indication of cases when the manufacturer is not responsible for the defect (e.g. the defect did not exist at the time of receipt of the goods in circulation or modern knowledge at that time could not predict the defect), and when liability can be reduced. The notion of presumed reasonable use of the product and negligence issues, such as the user's disregard for downloading the required security update, need to be clarified. The developed legal framework should ensure the availability of the necessary technical expertise, the cooperation of the potentially responsible party so victims, having all the necessary evidence, can easily receive compensation for damage caused by defects. At the same time manufacturers have the opportunity to take out affordable insurance to provide compensation regardless of their solvency reduce the cost of losses [2, p. 13-16].

There are still a number of pressing issues related to AI technology that need to be regulated. These include the protection of personal data, the regulation of business activities for the production of robots or software, copyright in works created by artificial intelligence, the role of AI in the dissemination of false information and unwanted content.

Artificial intelligence technologies will contribute to the transformation of the economy, labour market, government institutions and society as a whole. The use of artificial intelligence technologies will reduce costs, increase production efficiency, quality of goods and services. Ukraine has approved an AI Development Concept from 2 December 2020 , but it does not fully address such important issues as personal safety and responsibility to consumers. Ignoring these issues can lead to public rejection of new digital technologies and hesitation about their use. Therefore, it is necessary to consistently implement the legal provisions of the EU to national legislation not only to create conditions for the use of AI technologies, but also to ensure the safety of consumers using products and services with AI systems.

References:

1. CMU. (2020). *Order of the Cabinet of Ministers of Ukraine «On approval of the Concept of development of artificial intelligence in Ukraine»*. Official website of the Verkhovna Rada of Ukraine, December 2. Available at: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#n8

2. EC. (2020). *REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE «Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics»*. Official website of the European Commission, February 19. Available at: https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en

Водько Юлія

Студентка, КПІ ім.Ігоря Сікорського

ПОРІВНЯЛЬНО-ПРАВОВІ АСПЕКТИ ДОСЛІДЖЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ ТА ЗАКОНОДАВСТВА ДЕРЖАВ ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Питання забезпечення кібербезпеки держави щоразу стає все актуальнішим, зважаючи на масштабну та безупинну цифровізацію усіх сфер нашого життя. Захищеність важливих сфер державної діяльності, надання адміністративних

послуг, приватної коресподенції та будь-якої іншої сфери обігу інформації є надзвичайно гострою проблемою, а особливо у світлі гібридної війни Російської Федерації проти України. Зміни у законодавстві України пов’язані здебільшого з євроінтеграційним шляхом нашої держави, тож розглянемо проблеми регулювання забезпечення кібербезпеки у порівнянні із законодавством держав Європейського Союзу.

Варто наголосити на тому, що дослідження питань, що пов’язані із забезпеченням кібербезпеки повинно бути комплексним. Це означає те, що окремі законодавчі акти потрібно розглядати крізь призму практичних ситуацій діяльності державних органів, їх реагування на порушення та застосування методів убезпечення від загроз, що виникають у кіберпросторі та мають величезний вплив на всю інформаційну систему України.

Насамперед для того аби дослідити законодавство про кібербезпеку слід визначитися з системою понять, які є основою для подальшого розуміння теми. З позиції законодавства України визначення кіберзпезпеки звучить як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [1].

Що ж до тлумачення поняття кібербезпеки законодавством інших держав, то звернемося до праці Баранова О.А., в якій проаналізовано це питання. Отже, наведемо приклади тлумачень у законодавстві країн Європейського Союзу. Стратегія кібербезпеки Франції містить наступне визначення: кібербезпека – це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов’язаних з ними послуг, які ці системи пропонують або роблять доступними [2, с. 55].

У порівнянні з визначенням у національному законодавстві більше уваги приділено загальному стану інформаційної системи, а не лише кіберпростору. Тобто ці два поняття розглядаються як взаємопов’язані і поняття інформаційної системи – більш широко – як сфера, на яку мають вплив процеси, що відбуваються у кіберпросторі. Також у визначенні українського законодавства на відміну від французького виокремлено інтереси людини і громадянина, суспільства і держави, а також інтереси національної безпеки як об’єкти впливу потенційних загроз з боку кіберпростору. На нашу думку, слід проаналізувати доцільність обмеження поняття такою конкретизацією.

У німецькій стратегії під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків. Що ж до нідерландської Національної стратегії кібербезпеки, на думку авторів стратегії, кібербезпека – це сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі ІКТ або неправильного їх використання, а також з відновлення ІКТ після реалізації цих загроз [2, с. 55-56].

На нашу думку, ключова відмінність між проаналізованими дефініціями кібербезпеки є у тому, що в українському законодавстві це питання розглядається в межах питання забезпечення національної безпеки України та як його складова. А тому увага вирішенню цієї проблеми знаходить своє місце поряд з іншими елементами забезпечення національної безпеки України та покладена на державні органи, які здійснюють свої функції у цій сфері.

Для того аби розуміти динаміку розвитку галузі кібербезпеки необхідно звернути увагу на авторитетне міжнародне дослідження у цій сфері. За Національним індексом кібербезпеки (NCSI) (глобальний індекс, який вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами) станом на 2021 рік до першої десятки країн з найвищим рейтингом входять Греція, Чехія, Естонія, Литва, Іспанія, Польща, Бельгія, Фінляндія, Франція, Словаччина [3]. Україна наразі посідає 25 місце зі 193 можливих, що вище на три сходинки порівняно з позицією у 2019 році та аж на 34 позиції вище, ніж у 2017 році [4]. Таким чином можемо підкреслити позитивну динаміку у впровадженні різноманітних заходів щодо забезпечення кібербезпеки. Зазначається, що під час розробки нової редакції експерти аналізували такі напрямки: законодавство у сфері кібербезпеки, аналіз кіберінцидентів, освіта у сфері кібербезпеки, забезпечення захисту цифрових та основних послуг, електронна ідентифікація та довірчі послуги, захист персональних даних, заходи із реагування на кібератаки та кіберінциденти, боротьба із кіберзлочинністю. У Службі, що займається дослідженням NCSI, зазначають, що покращити позиції України вдалося завдяки ухваленим протягом останнього року законодавчим актам у галузі кібербезпеки та кіберзахисту [5].

В оглядовому звіті Комітету з питань трансформації, що стосується аналізу кращих практик управління кібербезпекою можемо знайти деякі висновки аналізу законодавства країн Європейського Союзу.

Зокрема про те, що Франція вдруге посіла друге місце в Європі, при цьому набрала 100 відсотків за категоріями правових та організаційних заходів. Франція активно співпрацює з інституційними партнерами (міністерствами, національними органами влади, приватним сектором та неприбутковими організаціями), а під час

Європейського місяця кібербезпеки використовує різні засоби для підвищення в суспільстві обізнаності з цих питань.

Литва ж має найвищий бал як у правовій, так і в організаційній категорії. Закон Литви про кібербезпеку містить положення, що дозволяють компетентним органам вживати заходів проти загальнодоступної інфраструктури електронного зв'язку, яка бере участь у шкідливій онлайн-діяльності. Державна інспекція захисту даних може публікувати інформацію про випадки, пов'язані з порушеннями персональних даних [6].

Підсумовуючи, можемо зробити висновок, що найбільш дієвою для вдосконалення національного законодавства у сфері кібербезпеки буде імплементація досвіду та кращих практик країн ЄС і стандартів НАТО з урахуванням умов Угоди про асоціацію між Україною. В українському законодавстві досить стрімко розробляються різні нормативно-правові акти, які спрямовані на забезпечення кібербезпеки, проте на нашу думку найголовніше аби ці зміни супроводжувалися ефективним впровадженням механізмів на практиці, оскільки вимірювання критеріїв захищеності кіберпростору та загалом інформаційної системи України відбувається у тісному взаємозв'язку з реальною, а не декларативною дією положень законодавчих актів.

Література:

1. Про основні засади забезпечення кібербезпеки: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 26.04.2021).
2. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». Журнал «Правова інформатика», № 2(42)/2014, с. 54-62. – URL: http://ippi.org.ua/sites/default/files/14boavpk.pdf (дата звернення: 26.04.2021)
3. Глобальний індекс кібербезпеки, 2021. URL: https://ncsi.ega.ee/ncsi-index/ (дата звернення: 26.04.2021)
4. ITU Global Cybersecurity Index (GCI) 2017: Глобальний індекс кібербезпеки. URL. https://www.itu.int/dms_pub/itu-d/opb/str/D-STRGCI.01-2017-R1-PDF-E.pdf (дата звернення: 26.04.2021)
5. Україна посіла 25 місце серед 160 країн у міжнародному рейтингу кібербезпеки. *Державна служба спеціального зв'язку та захисту інформації України*. 04.12.2020. URL: https://cutt.ly/yboXGSa (дата звернення: 26.04.2021)
6. Олексюк Л. Кращі практики управління кібербезпекою. Оглядовий звіт Комітету з питань цифрової трансформації. URL: https://www.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cybersecurity_04.pdf (дата звернення: 26.04.2021)

Войтко А.

студентка 1 курсу магістратури,
КПІ ім. Ігоря Сікорського
Науковий керівник: Радзієвська О. Г.
к.ю.н., старший дослідник, провідний
науковий співробітник ДНУ «Інститут
інформації, безпеки і права НАПрН України»

ПРАВОВІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У НАЦІОНАЛЬНОМУ ЗАКОНОДАВСТВІ ТА ЄВРОПЕЙСЬКОМУ ПРАВІ

У зв’язку з зростанням тенденцій до діджиталізації суспільства та переведення значної кількості операцій в режим онлайн, дедалі інтенсивнішого використання технологій блокчейн та Інтернету речей, питання захисту персональних даних при їх передаванні та обробці набуває все більшого значення. Правове забезпечення захисту персональних даних стає одним із найбільш актуальних та важливих напрямів державної політики, щодо створення безпечних умов для обробки даних громадян у сучасному цифровому світі. Ретроспективно розглядаючи питання захисту персональних даних важливо звернути увагу на те, що ще у 1960-х роках, коли почали з’являтися інформаційні технології, виникла потреба у розробці детальних правил щодо захисту даних осіб задля їх безпеки та уникнення неправомірних маніпуляцій з ними. У 70-х роках Комітетом міністрів Ради Європи були прийняті ряд резолюцій про захист персональних даних, які базувалися на статті 8 Конвенції про захист прав людини і основоположних свобод. У 1981 році Радою Європи була прийнята Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних. Ця Конвенція покликана була захистити особу від зловживань, які могли виникати при збиранні та обробці персональних даних, а також врегулювання шляхів транскордонної передачі персональних даних. Україна ратифікувала Конвенцію в 2010 році, що дає підстави припустити, що система дій спрямованих на захист персональних даних в Україні і в Європейському Союзі (ЄС) була подібною і будувалася на схожих принципах [1]

Вважається, що Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних – це перший міжнародний юридично зобов’язальний документ, який стосується виключно питань захисту персональних даних.

До 2016 року основним правовим інструментом ЄС у сфері захисту персональних даних була Директива 95/46/ЄС Європейського парламенту та Ради Європи від 24 жовтня 1995 року «Про захист фізичних осіб при обробці

персональних даних і про вільне переміщення таких даних». Зважаючи на те, що основною метою створення ЄС було вільне переміщення товарів, капіталів, послуг і осіб на внутрішньому ринку, то така діяльність вимагала вільного потоку даних, який не можна було б здійснити, якби держави-члени не могли розраховувати на однаково високий рівень захисту персональних даних. У зв’язку з цим постало питання розробки нормативно-правових актів, які були б універсальними та могли б застосовуватися до всіх держав-учасниць.

Директива 95/46/ЄС була скасована та замінена Регламентом Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, який визначив загальні умови передачі персональних даних, яких мають дотримуватися як держави-резиденти ЄС, так і нерезиденти.

Регламент 2016/679 не містить визначення поняття переміщення чи його особливостей. Контекст, у якому вживається поняття переміщення як операції з персональними даними вважається одним із прикладів розкриття персональних даних і тлумачиться як спосіб надання доступу до них.

Відповідно до Регламенту 2016/679, транскордонне передавання персональних даних до третіх країн або міжнародних організацій може відбуватися виключно на підставі:

- рішення Європейської Комісії про відповідність рівня захисту, який третя країна надає персональним даним, які передаються на її територію;
- ухвалених Європейською Комісією або відповідним наглядовим органом стандартних положень щодо захисту персональних даних;
- затверджених відповідним наглядовим органом зобов’язальних корпоративних правил;
- затвердженим кодексом поведінки у сукупності з наданими контролером чи обробником у третій країні зобов’язаннями застосувати належні гарантії щодо забезпечення прав суб’єктів даних;
- положень договору між контролером або оператором та контролером, оператором або одержувачем персональних даних у третій країні чи міжнародною організацією за наявності спеціального дозволу наглядового органу;
- затвердженим механізмом сертифікації у сукупності з наданими контролером чи обробником у третій країні зобов’язаннями застосувати належні гарантії щодо забезпечення прав суб’єктів даних.

На жаль, Україна поки не входить у список країн, які надають достатні гарантії захисту персональних даних, тому їх передавання дозволяється лише за однієї з таких умов:

- суб’єкт даних надав чітку згоду на запропоноване передавання після того, як його було повідомлено про можливі ризики такого передавання;
- передавання є необхідним для виконання контракту між суб’єктом даних і контролером, або реалізації переддоговірних заходів, вжитих на запит суб’єкта даних;
- передавання є необхідним для укладення чи виконання договору, укладеного в інтересах суб’єкта даних між контролером та іншою фізичною чи юридичною особою;
- передавання є необхідним для формування, здійснення або захисту правових претензій;
- передавання є необхідним на важливих підставах суспільного інтересу;
- передавання є необхідним для захисту життєво важливих інтересів суб’єкта даних або інших осіб, якщо суб’єкт даних фізично чи юридично неспроможний надати згоду. [2]

Порівнюючи українське законодавство із законодавством ЄС варто зауважити наступне: відповідно до ч. 1 ст. 32 Конституції України не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. [3]

З метою забезпечення незалежності уповноваженого органу з питань захисту персональних даних, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини. [4] Така ж практика присутня у країнах ЄС, зокрема в Федеративній Республіці Німеччини існує інститут Уповноваженого, діяльність якого регламентується положеннями Федерального Закону "Про подальший розвиток обробки і захисту даних" від 20.12.90 р. [5] Важливо звернути увагу на те, що згідно з ст. 15 Угоди про асоціацію між Україною та Європейським Союзом сторони домовились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема тих, що відповідають вимогам відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, inter alia, обмін інформацією та експертами. [6]

Таким чином, законодавство України та ЄС мають багато спільного та базуються на принципах закладених у Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних. Окрім того, Україна перебуває зараз в процесі гармонізації законодавства відповідно до законодавства ЄС та

здійснює транскордонну передачу персональних даних відповідно до Регламенту 2016/679. Це свідчить про те, що з метою транскордонної передачі даних, держави мають забезпечити їх контрагентам однакові умови та рівний захист інформації.

Діджиталізація є фактором який позитивно сприяє як розвитку бізнесу, так й економіки держави. Це допомагає заощадити час і підвищити продуктивність, шляхом автоматизації виробництва та інших внутрішніх процесів компанії, можливостями збільшення клієнтської бази, яка не прив’язана до конкретного місця та заохоченням клієнтів до придбання більшої кількості продукції. Варто зауважити, що Україна також здійснює кроки щодо діджиталізації сфери надання державних послуг, зокрема шляхом створення е-сервісів. Прикладом такого сервісу є додаток «Дія», розроблений Міністерством цифрової трансформації України. Окрім того, зважаючи на тенденції, які існують на сьогоднішній день, стан бізнесу напряму залежить від обмежень, спричинених пандемією Covid-19. Тому застосування дедалі більшої кількості сучасних технологій у компаніях є вже не лише їх бажанням, а швидше необхідність, без якої подальше функціонування всього бізнесу ставиться під сумнів.

У зв’язку з викладеним діяльність держави у сфері захисту персональних даних займає сьогодні одне з провідних місць. На думку автора, питання правового забезпечення захисту персональних даних є актуальними та потребують подальшого удосконалення через безкордонний потік інформації та переведення дедалі більшої кількості операцій в онлайн режим. Нормативно-правова база, яка регулює захист персональних даних в Україні сьогодні є недостатньо врегульованою, що суттєво обмежує можливості громадян та держави протидіяти спробам незаконного поширення такої інформації. У зв’язку з цим існує необхідність створення та розробки дієвого механізму захисту персональних даних, який унеможливить їх поширення. Доцільно було б розробити відповідно до вимог встановлених ЄС типове положення про транскордонну передачу даних, що сприятливо відображалося б на бізнесі та значно заощаджувало час.

Література:

1. Посібник з європейського права у сфері захисту персональних даних [Електронний ресурс]. – 2014. – Режим доступу: https://rm.coe.int/16805966a8**.**

2. Регламент Європейського Парламенту І Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [Електронний ресурс]. – 2016. – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text**.**

3. Конституція України [Електронний ресурс]. – 1996. – Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

4. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних [Електронний ресурс]. – 2013. – Режим доступу: https://zakon.rada.gov.ua/laws/show/383-18#Text.

5. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних [Електронний ресурс]. – 2006. – Режим доступу: https://just.odessa.gov.ua/files/upload/files/24.pdf.

6. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс]. – 2014. – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_011#Text.

Геворкян Л. А.

Студентка, КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ВИЗНАЧЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КОНТЕКСТІ ІНТЕРНЕТ РЕЧЕЙ

В останні роки у розвитку Інтернет-сфери набуває активного поширення словосполучення «Інтернет речей». Як зазначається у понятті «Інтернет речі» розглядається як фізично реальні системи і комплекси, функціонування яких базується на використанні величезної кількості датчиків, комп’ютерних і телекомунікаційних технологій, робототехніки, штучного інтелекту, хмарних обчислень, мережі Інтернет, застосування яких надає можливості за участю або без участі людей приймати і реалізовувати рішення. Завдяки інтернету задовольняються інформаційні, економічні та інші потреби. З появою ІТ у людства з’явились великі можливості, але з приходом можливостей приходить і велика відповідальність. З’явилась потреба в ефективному правовому регулюванні, що забезпечить безпечне використання ІТ по всьому світу. Метою даної роботи є розгляд можливих проблем правового регулювання в умовах застосування технологій інтернету речей та пошук можливих рішень.

На думку Баранова О.А. під «Інтернетом речей» варто розуміти комплекси і системи, що складаються з сенсорів, мікропроцесорів, виконавчих пристроїв, локальних та / або розподілених обчислювальних ресурсів і програмних засобів, програм штучного інтелекту, технологій хмарних обчислювань, передача даних між

якими здійснюється за допомогою мережі Інтернет, та які призначені для надання послуг і проведення робіт в інтересах суб'єктів (юридичних або фізичних осіб) [2, с. 9].

Інтернет речі, це як система, що об’єднує матеріальні речі (фізичні) за допомогою мережі Інтернет завдяки чому Інтернет речей може глобально вплинути на розвиток суспільства знань та дозволить численним процесам відбуватися без участі людини. Лідерами у розробці та впровадженні Інтернету речей є країни, в яких розвинена індустрія виробництва мікропроцесорів та вбудованих комп'ютерів — США, Китай, Південна Корея, крім того прогрес у цій галузі демонструють європейські країни та Японії.

На даний момент не існує ефективного, єдиного методу ідентифікації конкретних осіб причетних до незаконних діянь що призвели до втрати персональних даних конкретної особи. Адже лише використання проксі-серверів вже робить користувача анонімним. Згідно основоположних принципів міжнародного права про захист персональних даних, затвердженими першою у світі Конвенцією Ради Європи № 108 від 28.01.81 р. та рядом директив Європейського Союзу, зокрема Директивою Європейського Парламенту і Ради 95/46/ЄС від 24.10.95 р., стосовно захисту персональних даних, захист прав людини у сфері персональних даних передбачає, зокрема, наступне: «Персональні дані, що піддаються автоматизованій обробці: a) отримуються та обробляються сумлінно та законно; b) зберігаються для визначених і законних цілей та не використовуються у спосіб, несумісний з цими цілями; c) мають бути адекватними, відповідними і не надмірними з точки зору цілей, для яких вони зберігаються». [1, с. 75]

Близько 8 років тому була створена перша криптовалюта світу «біткоїн». Специфічна природа криптовалюти зумовлює те, що відповідне питання не є першочерговим для вирішення. Але необхідність втручання держави в особі її органів була зумовлена тим, що біткоїн став платіжним засобом діяльності Даркнету, анонімна мережа, яка на сьогодні активно функціонує в мережі Інтернет по всьому світу, яка схожа на чорний ринок, де можна придбати зброю, наркотики, людей, фальшиві гроші та документи. США, Німеччина, Японія, Франція, Фінляндія та інші країни не тільки дозволили обіг відповідної валюти, але й законодавчо закріпили чи підкріпили правовий режим, роз’яснили поняття біткоїнів та аналогів сформували відповідну судову практику. Чимало держав все-таки не встановлює режиму щодо криптовалюти через її специфічну природу. До таких держав відноситься і Україна. Проблемою, яка є найбільш фундаментальною і очевидною, є правова природа криптовалюти. [3, с. 105]

Нині технології Інтернет речей впроваджені у традиційні закриті та обмежені для розголосу інформаційні простори, тобто у наше приватне життя. Поступово зростаючи, за кількістю датчиків, будуть ще більше збирати даних про людину, тому широке застосування технологій Інтернет речей робить актуальним питання контролю, узгодження та прозорості щодо розмежування між приватним й суспільними сферами. [6, с. 75].

З вище описаного можна зробити висновок, що на міжнародному рівні сьогодні відсутня єдність в розумінні правової природи криптовалюти, тому держави по-різному визначають поняття біткоїна і його аналогам. Європейська судова практика по суті прирівняла криптовалюту до законного платіжного засобу, а обмін грошових коштів – «валютно-обмінною операцією». Але все-таки, згідно чинного законодавства ЄС цифрова валюта вважається товаром і підпадає під регулювання Цивільного законодавства і Директиви ЄС про ПДФ як товар, а договір купівлі–продажу щодо криптовалюти є договором купівлі–продажу товару [4,с. 14]. Щодо застосування штучного інтелекту, необхідно буде вирішити дуже багато правових проблем в регулюванні пов’язаних з тією обставиною, що людина – біологічна істота, а робот – ні. Перш за все, це проблеми визначення для роботів понять, критеріїв, змісту та обсягів правоздатності, дієздатності і деліктоздатності; вирішення проблеми встановлення для роботів спеціальної або загальної правосуб’єктності і багато інших. Іншими словами, роботи розглядаються як людиноподібні суб'єкти, які здійснюють людиноподібні дії в процесі відносин з традиційними суб'єктами. Якщо дії традиційних суб'єктів в таких відносинах підлягають правовому регулюванню, то логічно припустити, що інша сторона також є суб'єктом цих правовідносин. Якщо робот-андроїд або андроїд повинен нести юридичну відповідальність за свої дії, тоді він повинен мати фізичну, юридичну та цифрову ідентичність, подібну людині. І якщо у робота є ті ж юридичні обов’язки, що і у людини, хіба в нього не повинні бути такі ж юридичні права, як у людини? [4, с. 10].

Підкреслюючи вищесказане, можна стверджувати що без чіткого механізму правового регулювання, сучасні технології перетворять наше життя на хаос, за яким може прийти не тільки стагнація, але й війна. Завершити хотілося б словами Річарда Хукера, які як ніколи описують розвиток сучасних технологій: «Будь-яка зміна, навіть зміна на краще, завжди пов’язана з незручностями» [3, с. 120].

Література:

1. Баранов О.А. Захист персональних даних в сфері Інтернет речей: 2017. 85-91 с.

2. Баранов О. А. Захист інтернет речей: Огляд правових проблем Інтернет речей та проблеми правового регулювання: Київ, 2017 . 237с.

3. Брижко В.М Чему угрожает будущее. URL : http:// igate.com.ua/news/31 69-internet-veshhej-chem-ugrozhaet-budushhee (Дата звернення 26.04.21).

4. Пилипчук В.Г. Захист Інтернет речей: проблеми правового регулювання та впровадження / Становлення і регулювання суспільних відносин у сфері новітніх інформаційних технологій: 2017. 17 с.

5. Плита А.І. Есе з права ІТ криптовалюта та її правовий режим: 2017. 2-7 абзац.

Геращенко Яна

Студентка, КПІ ім. Ігоря Сікорського

«ДЕРЖАВА У СМАРТФОНІ»: ШЛЯХ ДО ПОВНОЇ ЛЕГАЛІЗАЦІЇ ЕЛЕКТРОННИХ ПАСПОРТІВ ТА СУЧАСНИЙ СТАН ПИТАННЯ

Цифрова трансформація охоплює все більше сфер нашого життя. Вплив сучасних технологій сьогодні на собі може відчути кожен українець, адже мабуть не залишилося того, хто не робив би спроби користуватися перевагами додатку «ДІЯ» або ж бодай не чув про нього.

Хоча сервіс «Держава і Я» (скорочено «ДІЯ») є дійсно молодим, адже його запуск відбувся лише 16 грудня 2019 року – він встиг наробити галасу та отримати неабияку популярність серед населення. Застосунок вміщує немалу кількість електронних документів, які підвантажуються автоматично з реєстрацією, зокрема це водійське посвідчення, студентський квиток, закордонний паспорт, реєстраційний номер облікової картки платника податків тощо. Центральною фігурою додатку можна вважати основний документ кожного громадянина – паспорт.

Використання цифрового паспорту було спірним питанням протягом всього часу існування додатку, адже як громадянам так і суб’єктам, яким пред’являвся такий паспорт часто не вистачало усвідомлення правового статусу цього проекту, який, до речі, був на етапі експериментального. З підстав різнотлумачення правового регулювання електронного документообігу особистих документів громадян виникали конфлікти, спричинялись незручності, а переваги такої цифровізації вбачались вже не такими і актуальними.

Таким чином, основною проблемою для широкого та безперешкодного застосування цифрових паспортів є певна прогалина у правосвідомості таких застосувачів, які не до кінця розуміли сутність цього урядового експериментального проекту.

Крапку в цій ситуації невизначеності Верховна Рада України поставила 30 березня 2021 року, ухваливши у другому читанні законопроект №4355 «Про внесення змін до закону «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [1].

Таким чином, на законодавчому рівні було прирівняно електронний паспорт громадянина України та паспорт для виїзду за кордон у додатку «ДІЯ» до їх пластикових та паперових аналогів.

Шлях до цього був досить коротким, адже перші кроки у правовому регулюванні такої цифрової інновації було зроблено вже через пів року після офіційного запуску «ДІЯ». Відтак, Постановою Кабінету Міністрів України № 278 від 15 квітня 2020 року “Про реалізацію експериментального проекту щодо застосування відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, та відображення в електронному вигляді інформації, що міститься у паспорті громадянина України для виїзду за кордон, якою, зокрема, було затверджено Порядок застосування відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, та відображення в електронному вигляді інформації, що міститься у паспорті громадянина України для виїзду за кордон, під час реалізації експериментального проекту щодо застосування зазначених відображень.

Зазначений вище порядок, вводив в обіг поняття «е-паспорт» під яким розуміється відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, оформленому особі засобами Єдиного державного демографічного реєстру, разом з унікальним електронним ідентифікатором (QR-кодом, штрих-кодом, цифровим кодом тощо), який забезпечує отримання інформації з Реєстру інформаційними ресурсами єдиної інформаційної системи МВС на запит Єдиного державного веб-порталу електронних послуг “Портал Дія” [2].

Також, встановлювався порядок використання такого паспорту, визначалась інформація, яку він вміщував, особливості перевірки та підтвердження інформації про особу.

На той момент, пунктом 3 вказаного Порядку встановлювався виключний перелік випадків, в яких громадяни могли скористатися цифровим паспортом, що

імовірно випливало з того, що даний проект все ж був експериментальним, а тому сфера його дії була досить вузькою.

У зв’язку з цим громадяни не володіючи інформацією з приводу сфери застосування е-паспортів часто намагались довести свою правоту намагаючись використати цифровий паспорт «поза межами його дії» і отримували категоричну відмову. Це призводило до обурення і формування недовіри до додатку «ДІЯ», яка, як виявилось, не має аж такої користі у повсякденному житті, як цього обіцяв уряд.

Проте, 30 березня 2021 року мережа переповнилась новинами про прирівняння е-паспортів до їх реальних аналогів. Відтак, народні депутати прийняли Проект Закону про внесення змін до Закону України “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”. Зазначеним Законом передбачається ряд змін до чинного законодавства України спрямованих на легалізацію цифрового паспорту і перш за все остаточне закріплення поняття е-паспорту. Повне регулювання питання здійснюватиметься новою статтею 14-1 Закону України “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”; (Е-паспорт і е-паспорт для виїзду за кордон).

Варто зазначити, що Прикінцеві та перехідні положення зазначеного вище Закону передбачають, що цей Закон набирає чинності з 23 серпня 2021 року [1]. А отже, повноправно та безперешкодно користуватися перевагами е-паспорту можна буде лише наприкінці літа 2021-го. Цікаво, що Міністерство цифрової трансформації заявило, що наша країна стала першою у світі, яка узаконила таку цифровізацію. Відмітимо, що електронний паспорт став не першим документом, який був прирівняний до фізичного аналогу в Україні. У лютому 2021 р. Верховна Рада України узаконила електронні водійські права, які власне і стали першопроходьцем у сфері цифрової трансформації документообігу особистих документів громадян України.

Висновки. Додаток «ДІЯ» є досить багатогранним, адже станом на сьогодні він містить ще велику кількість експериментальних функцій, як от електронний студентський квиток, картка платника податків реєстрація місця проживання онлайн, профіль виборця тощо. Громадянам варто пам’ятати, що наразі безперешкодно можна користуватися лише трьома видами електронних документів: паспорт громадянина України, паспорт громадянина України для виїзду за кордон та водійське посвідчення – стосовно інших можливостей застосунку необхідно спершу ознайомитися з правилами їх використання, на які

сфери життя вони поширюються та які проблеми чи питання можуть виникнути у зв’язку з цим.

На перспективу, державна політика сьогодні спрямована на все більшу цифровізацію всіх сфер людської діяльності. Міністерство цифрової трансформації України активно працює над постійними оновленнями «ДІЯ» та робить все, аби в найближчі роки бюрократизм документообігу було повністю ліквідовано. Саме тому, можна говорити про великі перспективи «держави у смартфоні». Насправді, легалізація е-паспортів це лише перший крок до цифровізації численних сфер життя населення, пов’язаних із взаємодією громадянина з державою, її органами тощо.

Література:

1. Про внесення змін до Закону України “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”: Закон України № 1368IX від 31 березня 2021 року. URL:

https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70393 (дата звернення 26.04.2021 р.)

2. Порядок застосування відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, та відображення в електронному вигляді інформації, що міститься у паспорті громадянина України для виїзду за кордон, під час реалізації експериментального проекту щодо застосування зазначених відображень затверджений Постановою Кабінету Міністрів України від 15 квітня 2020 року №278 Про реалізацію експериментального проекту щодо застосування відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, та відображення в електронному вигляді інформації, що міститься у паспорті громадянина України для виїзду за кордон / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/278-2020-%D0%BF#Text (дата звернення 26.04.2021 р.)

Голіченко Дмитро
курсант ІСЗЗІ, КПІ ім. Ігоря Сікорського
Журбенко Данило
курсант ІСЗЗІ, КПІ ім. Ігоря Сікорського
Науковий керівник: Кубайчук О.О.,
к.ф.-м.н., доцент, професор спеціальної кафедри №1 ІСЗЗІ
КПІ ім. Ігоря Сікорського

СУЧАСНІ ТЕНДЕНЦІЇ ПРАВОВОГО РЕГУЛЮВАННЯ КРИПТОВАЛЮТ В УКРАЇНІ ТА СВІТІ

Світова економіка знаходиться в постійному стані трансформації, змінюються механізми регулювання і технологічні цінності. Цей процес прискорюється за рахунок появи глобальної цифровізації, яка вплинула на розвиток практично всіх сфер економіки.

В результаті з’явилися нові ринки, форми комунікацій, підходи до управління виробництвом товарів і надання послуг. У той же час обслуговування угод купівлі-продажу здійснювалося з використанням фіатних грошей і банківської інфраструктури. Поєднання цифрового середовища та аналогових способів оплати призводило до зниження швидкості і високої вартості транзакцій, а також появи ризику втрати грошових активів в результаті шахрайських дій третіх осіб.

Пошук вирішення проблем збігся зі світовою фінансовою кризою 2007-2009 років і дестабілізацією міжнародних економічних відносин через ускладнення умов торгівлі і введення економічних санкцій. У цих умовах став формуватися альтернативний інструмент заощадження накопичень і нових еквівалентів грошей, що відповідають сучасним вимогам цифрової економіки [1]. Поява криптовалюти стала справжньою технологічною відповіддю на ці виклики.

По суті, криптовалюта - це ланцюжок шифрованих даних, що створюються в процесі майнінгу, є складовою децентралізованої системи і дозволяють передавати їх без участі інших осіб. Використання криптовалют не вимагає зв’язку з центром, тому вартість транзакції мінімальна. Крім того, криптовалюти прості в регулюванні, так як підпорядковуються закону попиту і пропозиції, а не політиці держав.

Стрімкий розвиток і зростання масштабів використання технології блокчейн сформували актуальне завдання для державних регулюючих органів
по створенню певних правових рамок для даного феномена. Необхідність

правового регулювання криптовалют продиктована значною кількістю напрямів діяльності пов’язаних з ними, таких як робота біржових платформ, здійснення платежів та оподаткування у криптовалюті. Важливим чинником є функціонування принципів верховенства права. Оскільки навіть якщо в державі
реалізоване законодавство, що сприяє розвитку блокчейну, але правові інститути досить слабкі, то це спричиняє великі ризики для інвестицій та
бізнесу [2].

Більшість передових країн вже досить завзято намагаються застосовувати блокчейн у державній економіці. Юридичний статус віртуальних валют значно відрізняється по всьому світу. У ряді країн операції з ними офіційно дозволені.

Зазвичай вони розглядаються як інвестиційний капітал або звичайний товар задля здійснення їх оподаткування. У даний час у світі відсутня нормативно-правова база, що встановлює еталонні правила. Проте вже зараз в деяких країнах йдуть спроби включення криптоінвестування в правове поле і надання криптовалюті офіційного статусу [3].

До прикладу, Японія є першою з країн, що прирівняла цифрові гроші до реальних та легалізувала криптобіржі, розробивши правила їх діяльності. В той же час криптовалютні компанії вимушені сплачувати податок на споживання від продажу криптовалют, оскільки такі доходи класифікуються як “інший дохід”.

Швейцарія належить до переліку країн, де операції з криптовалютами є законними. Криптовалюта – це актив, що обкладається податком на майно, а її власники зобов’язані подавати щорічні фінансові декларації. Держава створює всі необхідні умови для інтеграції криптовалюти в фінансову систему країни.

Великобританія відноситься до країн, де юридичний статус криптоіндустрії є нейтральним. Місцеві біржі та обмінники зобов’язані проходити державну реєстрацію в Управлінні з фінансового регулювання і нагляду, проте сама криптовалюта досі неузаконена.

У Китаї будь-які операції з криптовалютою та діяльності криптобірж є забороненими. Крім того, місцевою владою заохочуються донесення на тих, хто
пов’язаний з криптовалютним трейдингом та заробляють завдяки перепадам
цін.

У Сполучених Штатах Америки здійснюється надмірне регулювання діяльності, пов’язаної з криптовалютами, що ускладнює ведення бізнесу. Державна комісія з цінних паперів і бірж розцінює цифровий актив як цінні папери. Приватні особи та компанії вказують на продаж, обмін криптовалюти
та оплату товарів за неї у податковому звіті. Але, не дивлячись на бюрократичні складнощі, США залишаються лідером за кількістю блокчейн-компаній [4].

Для створення ефективного механізму правової регламентації засобів криптовалюти в Україні необхідно враховувати досвід зарубіжних країн, застосовувати їх технології, але з адаптацією до українських економічних і правових реалій.

Україна наразі входить до ТОП-10 країн світу за кількістю користувачів біткоїна. І хоч у нашій країні функціонує велика кількість крупних девелоперських та дослідницьких компаній, а також досить розвинуте криптовалютне співтовариство, проте правовий статус криптовалюти та суспільних відносин у сфері їх застосування досі є не визначеним.

Невирішеним залишається і питання оподаткування криптовалютних операцій. Оскільки будь-які спеціальні норми є відсутніми, до них застосовуються стандартні правила оподаткування. Так, прибуток фізичної особи, отриманий у вигляді цифрової валюти, оподатковується за стандартною ставкою 18%.

Але варто розуміти, що визнання криптовалюти, та загалом технології блокчейн, на законодавчому рівні може досить істотно трансформувати українську економіку та сприяти становленню України як цифрової держави. Саме тому, найближчім часом очікуються сприятливі тенденції щодо
даної перспективи. У грудні 2020 року Верховною Радою України у першому читанні було прийнято за основу проект Закону «Про віртуальні активи», який регламентує їх переведення до правової площини. Наразі документ готується на друге читання. З його ухваленням, правовідносини в сфері криптовалют визначатимуться як ринок віртуальних активів, що відповідає світовій реалізації регулювання цієї сфери. Міністерство цифрової трансформації, в даному випадку, стане регулятором ринку, а Національний банк України чи Національна комісія з цінних паперів та фондового ринку — його ліцензіаром. Після легалізації цього ринку в Україні, організації зможуть офіційно вивести віртуальні грошові операції на відкриту площину та залучати іноземні інвестиції, а українські фахівці з блокчейну – розвивати свої проекти. Закон
“Про віртуальні активи” сприятиме усуненню ризиків для світових компаній, а користувачі зможуть прозоро декларувати свої доходи у криптовалюті [5].

Зареєстровані криптообмінники та біржі ідентифікуватимуть та ізолюватимуть чисту криптовалюту від тієї, що була задіяна у грошових потоках з відмиванням грошей, фінансуванням тероризму та іншими злочинами. Така практика відстежування витіснить нелегальні криптоактиви з регульованого ринку віртуальних активів, а обіг криптовалюти, що перебуває поза легальним середовищем, буде підпадати під відкрите порушення закону.

Крім цього ці нормативно-правові зміни дозволять блокувати підозрілі транзакції. Державне регулювання захистить майнерів від вилучень обладнання силовими структурами і надасть доступ до банківських послуг. Питання податкового декларування доходів будуть вирішені в наступному законопроекті про внесення змін до Податкового кодексу України, розробка якого можлива тільки після повного прийняття базового закону України “Про віртуальні активи”[6].

Отже, кожна країна законодавчо регулює правовідносини у сфері криптовалюти по-різному з певними специфікаціями. І хоча кожне законодавство є особливим, спостерігається синхронізація у певних базисних положеннях, таких як ідентифікація користувачів або фінансовий моніторинг.

Задля утвердження та контролю ринку віртуальних активів Україною було обрано стратегію розробки спеціального законодавства. Таким чином буде створене таке юридичне середовище, що посприяє збільшенню інновацій у державі, а для роботи компаній і підприємців будуть створені комфортні умови. У довгостроковій перспективі легалізація криптовалютного ринку спонукатиме розвитку української економіки, що може призвести до справжнього цифрового перевороту й допоможе інтегруватись до світової економічної спільноти.

Література:

1. Криптовалюты и блокчейн как атрибуты новой экономики: доклад Евразийской экономической комиссии, 24 апреля 2019 г. Москва: ЕЭК, 2019. 90 с. URL: http://www.eurasiancommission.org/ru/act/integr_i_makroec/dep_makroec_pol/ SiteAssets/%D0%94%D0%BE%D0%BA%D0%BB%D0%B0%D0%B4.pdf (дата обращения: 25.04.2021).

2. Правовое регулирование криптовалютного бизнеса: отчет Axon Partners и ForkLog Research, февраль 2017 г. Киев: Axon Partners, 2017. 101 с. URL: https://axon.partners/wp-content/uploads/2017/02/Global-Issues-of-Bitcoin- Businesses-Regulation.pdf (дата обращения: 25.04.2021).

3. Доронін І. М. Блокчейн, суспільство і держава: проблеми правотворчості. ІТ-право: проблеми та перспективи розвитку в Україні: зб. матер. ІІ Міжнар. наук.-практ. конф., 17 листоп. 2017 р. Львів: НУ «Львівська політехніка», 2017. URL: http://aphd.ua/publication-359/ (дата звернення: 25.04.2021).

4. Дем’янюк М. Як у світі регулюють криптовалюти і коли цього очікувати в Україні Українська правда: веб-сайт. URL: https://www.epravda.com.ua/columns/2020/12/1/668690/ (дата звернення: 25.04.2021).

5. Проект Закону про віртуальні активи. Верховна рада України: веб- сайт. №3637. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110 (дата звернення: 25.04.2021).

6. Розвінчуємо міфи про законопроект «Про віртуальні активи». Міністерство та Комітет цифрової трансформації України: веб-сайт. URL: https://thedigital.gov.ua/news/rozvinchuemo-mifi-pro-zakonoproekt-pro-virtualni- aktivi (дата звернення: 25.04.2021).

Гречко Ярослава
студентка КПІ ім. Ігоря Сікорського
Науковий керівник: Головко О. М.,
к.ю.н., старший викладач
кафедри публічного права
КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН ПРИ ВИКОРАСТАННІ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасний науково-технічний прогрес передбачає ефективне розв’язання проблем шляхом інтеграції у суспільне повсякденне життя технологічних напрацювань. Алгоритми діяльності штучного інтелекту (далі – ШІ) оточують нас у всіх сферах діяльності, оскільки, на відміну від людей, функціональні елементи ШІ мають надзвичайно малий розмір і гранично мале енергоспоживання, що надає їм можливість працювати безперервно і залишатися непоміченими. Незважаючи на відносну новизну ШІ, міжнародне законодавство регламентує і регулює його використання. Щодо національного законодавства, Україна довгий час не мала нормативних актів, які б регулювали сферу штучного інтелекту, а законодавство щодо захисту персональних даних було недосконалим. Проте у 2020 році у Міністерстві цифрової трансформації було створено комітет цифрової трансформації, який за близько 9 місяців роботи опублікував Концепцію розвитку штучного інтелекту в Україні (далі – Концепція), яка визначає напрями діяльності, проблеми та шляхи подолання технологій штучного інтелекту в Україні на основі Керівних принципів

Організації економічного співробітництва і розвитку з питань штучного інтелекту, до якої Україна приєдналася в 2019 році. Щодо основних принципів, то штучний інтелект має приносити користь людям і планеті, сприяючи розвитку та добробуту; системи штучного інтелекту розробляються та використовуються лише за умови дотримання верховенства права, а їх використання має забезпечуватися відповідними гарантіями (можливістю безперешкодного втручання людини у процес

функціонування системи); забезпечення прозорості та відповідального розкриття інформації про системи штучного інтелекту; організації та особи, які розробляють, впроваджують або
використовують системи штучного інтелекту, несуть відповідальність за їх
належне функціонування [1].

Виокремлення саме цих позицій фундаментальним є не безпідставним, оскільки суспільна обізнаність у питанні штучного інтелекту та впровадження технологічних досягнень у життя загалом є низькою і до того ж обрамлена міфами: постійний прогрес,який досить швидко призведе до керування технікою людини; техніка заміщує людину в геометричній прогресії чи міф про те, що штучний інтелект зможе вирішити проблеми глобального світового масштабу. Примітно також зазначити, що дані принципи запропоновані текстом концепції Організації економічного співробітництва та розвитку (далі – ОЕСР), однак забезпечення тільки цих принципів для формування правових засад використання ШІ недостатньо для сучасних реалій України. Концепція визначає 8 напрямів державної політики, які покликані вирішити низку проблем щодо ШІ та вивести Україну на якісно новий рівень в системі світового розвитку штучного інтелекту.

Визначаючи перелік проблем та стратегії їх подолання досить позитивно, що було звернуто увагу як на соціальні фактори (такі як необізнаність населення) так і на економічні, що визначають готовність держави для розвитку та впровадження технологій ШІ. Основними завданнями в цих напрямках є :

1) Освіта і професійне навчання: підготовка кваліфікованих кадрів, зокрема через формування програм навчання цифрової грамотності серед школярів та освітні програм штучного інтелекту в межах галузі «Інформаційні технології» серед студентів, активне залучення педагогів до курсів з основ ШІ та роботи з даними; налагодження міжнародної співпраці та програм подвійних дипломів у сфері штучного інтелекту.

2) Наука: гарантування фінансування наукової діяльності у сфері штучного інтелекту, стимулювання наукових досліджень, співпраця з міжнародними науковими центрами для обміну досвідом; застосування досягнень ШІ у науковій діяльності.

3) Економіка: розвиток підприємництва (доступ інноваційних підприємств до інвестицій, поліпшення бізнес-клімату, партнерство з міжнародними організаціями), розроблення Дорожньої карти щодо перекваліфікації людей, робота яких може бути автоматизованою в найближчі роки.

4) Кібербезпека: захист комунікаційних, інформаційних та технологічних систем; удосконалення нормативно-правової бази щодо ШІ у сфері кібербезпеки та кіберзахисту, вивчення питання щодо можливості ліцензування іноземних розробок.

5) Інформаційна безпека: створення захищеного інформаційного простору за допомогою методів ШІ; виявлення, запобігання та викорінення можливих загроз.

6) Оборона: введення у використання ШІ в оборонних системах (збору та аналізу інформації під час бойових дій, обробка картографічної інформації та інше).

7) Публічне управління: автоматизація певних адміністративних послуг, дослідження та застосування ШІ у сфері охорони здоров'я, зокрема для моніторингу ситуації з пандемією та протидії їй. Варто зазначити, що у період пандемії можливість залучення технологій ШІ могла б спростити діяльність та аналізувати чи прогнозувати наслідки, тому доцільно було б медицину та охорону здоров'я виділити окремим та приорітетним напрямком реалізації державної політики.

8) Правосуддя: розвиток вже існуючих технологій, винесення судових рішень (за взаємною згодою сторін) на основі результатів аналізу, здійсненого ШІ.

Дана концепція для України - це перший крок у впровадженні та регулюванні технологій штучного інтелекту. Для більш чіткої стратегії її розвитку було б позитивно перейняти досвід міжнародної спільноти шляхом імплементації Етичного кодексу (створеного Європейською комісією) та доопрацювати керівні принципи діяльності і вже на їхній основі прийняти спеціальні нормативно-правові акти, що встановлюватимуть норми загальнообов'язкового регулювання окремих сфер використання технологій штучного інтелекту.

Література:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.20. № 1556-р./Кабінет Міністрів України. URL: https://www.kmu.gov.ua/npas/pro-shvalennya- koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220 (дата звернення 25.04.2021).

2. Карчевський М.В. Основні проблеми правового регулювання соціалізації штучного інтелекту. Вісник ЛДУВС.2017.№2. С.99-108. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03 =FILA=&2_S21STR=Vlduvs_2017_2_13 (дата звернення 25.04.2021).

3. Як Мінцифри бачить ШІ в Україні: аналіз концепції розвитку штучного інтелекту. 2020. URL: https://dslua.org/publications/yak-mintsyfry-bachyt-ai-v-ukraini-analiz-kontseptsii-rozvytku-shtuchnoho-intelektu (дата звернення 25.04.2021).

4. Мартинюк В.О. Правова регламентація використання штучного інтелекту. 2021. URL:http://www.er.ucu.edu.ua:8080/bitstream/handle/1/2604/Martyniuk_mag.pdf?seq uence=1&isAllowed=y (дата звернення 25.04.2021).

Данілевич Д. Р.

Студентка, КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ: ЙОГО ПРАВОСУБ'ЄКТНІСТЬ

Сьогодні сучасний світ перебуває на етапі швидкого розвитку та вдосконалення всіх сфер його суспільного життя. Науково-технічних прогрес став одним з ключових каталізаторів появи новітніх технологій. Безумовно, всі ці зміни є позитивними і сприяють розвитку, проте неможливо оминути увагою і проблемні питання, які виникають в ході експлуатації та використанні людиною новітніх Інтернет речей.

Одним із таких феноменів сучасності є штучний інтелект. Навколо самого поняття штучного інтелекту точаться багато дискусій і в результаті цього кожен вкладає в його зміст своє бачення. Перші трактування даного явища належать відомому американському інформатику Джону Маккарті, команда якого власне і є розробниками першого штучного інтелекту. Прийнято розуміти, що штучний інтелект являє собою певну здатність машини (комп'ютера), яка полягає у можливості виконувати різного роду завдання, які більшою мірою притаманні розумним істотам. [1] Доцільно буде зазначити, що це визначення є досить звуженим, тому пропонуємо розглядати його в більш широких рамках і визначати штучний інтелект як систему, яка розроблена і функціонує штучно, з притаманними їй близькими до людських здібностями, за допомогою яких вона може виконати будь-які реальні задачі і завдання, які перед нею ставляться.

Наявність багатьох трактувань самого поняття штучного інтелекту, як окремого виду Інтернет речей, говорить про те, що навколо нього існує ще і інший ряд до кінця нез'ясованих питань. Всі вони пов'язані з його правовою природою, правосуб'єктністю, питаннями користі і можливого ризику, існуванням чи навпаки відсутністю певного роду законодавчих норм, які спрямовуються на регулювання його існування та використання, а також ще

ряд нюансів, суміжних з вищезазначеними, які потребують дослідження та детального вивчення.

Розглянемо детальніше проблемний аспект, який пов’язаний з правосуб’єктністю штучного інтелекту, якому у своїх дослідженнях приділяли увагу багато науковців, проте кінцевого рішення і єдиної точки зору на сьогодні все ж не існує.

Цікавою і досить вагомою є позиція в даному питанні доктора юридичних наук Баранова О.А. Його наукова праця, що стосується правового регулювання та правосуб’єктності штучного інтелекту є вагомим внеском у розвиток даного питання. Професор підтримує позицію, висловлену Парламентом Євросоюзу, на рахунок необхідності закріплення на законодавчому рівні існування та функціонування всіх сучасних Інтернет речей, зокрема і штучного інтелекту, яке є необхідністю задля дотримання всіх вимог закону та етики. [2]

Також свої думки на рахунок правосуб’єктності штучного інтелекту виражали і вчені з Університету технологій МАРА. Їх думки направлені в сторону того, що «розумну техніку» можливо буде визнати в якості юридичної особи. [3] В результаті цього відбудеться покладання на неї всіх відповідних прав та обов’язків, що передбачаються законодавством.

Пропозиція визнати робота з штучним інтелектом юридичною особою, що одночасно означитиме і визнання його як суб’єкта права, безумовно є досить цікавою, проте неоднозначною. Фактично, робот і, відповідно, програма, яка є основою його діяльності, створюється людиною штучно. Це означає, що про свободу вибору у діях, які він вчиняє, як таку, говорити ми не можемо. Проте, науково-технічний прогрес не стоїть на одному місці і тому з упевненістю можна стверджувати і розглядати можливий варіант того, що рано чи пізно процес, який полягає у прийнятті роботом певного рішення, хоча і здійснюватиметься на основі штучно створеної програми, буде розглядатись вже як самостійний і незалежний акт його вольової поведінки.

Включення робототехніки зі штучним інтелектом до ряду суб’єктів права потребуватиме і внесення коректив до системи юстиції. У такому випадку ми можемо говорити вже про появу такого терміну, як до прикладу, «юстиція штучного інтелекту». [4] Достатньо вагомий, як на нашу думку, правовий важель в даній сфері, оскільки саме в рамках такого роду юстиції можливо буде вирішувати питання, які пов’язані з протидією роботам, у випадку їх загрози для добропорядку суспільних відносин, а також в цілому спорів, які будуть виникати в площині суспільство – робот.

Отже, роблячи висновок з вищеописаних позицій можемо однозначно сказати, що подальше успішне існування штучного інтелекту можливе лише за умови забезпечення повноцінної правової бази, визначення приналежності

робототехніки до суб’єктів права і можливості наділення їх правами та обов’язками . Звичайно, з плином часу і під впливом стрімкого розвитку технологій це питання буде однозначно вирішуватись, але ми вважаємо, що необхідно приділити увагу цьому вже зараз. Саме законодавче закріплення стане гарантом успішного удосконалення Інтернет речей, можливості інвестицій у розробку робототехніки та підвищення їх впливу у суспільних відносинах.

Література:

1. Encyclopædia Britannica (англ. British Encyclopaedia, укр. Британська енциклопедія) URL: https://www.britannica.com/search?query=artificial+intelligence

2. Баранов, О. А. (2017). Інтернет речей і штучний інтелект: витоки проблеми правового регулювання: зб. матеріалів II-ї міжнародної науково-практичної конф. IT-право: проблеми та перспективи розвитку в Україні, 18-42. URL: http://aphd.ua/publication-249/.

3. Willick, S. (1983). Magazine N, 4(2), 5-16.

4. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія / Н. А. Савінова. URL: http://ippi.org.ua/ udoskonalennya- kriminalno-pravovogo-zabezpechennya-rozvitku-informatsiinogo-suspilstva

Добровольська А.Ю.

Студентка, КПІ ім. Ігоря Сікорського

БЛОКЧЕЙН ІНІЦІАТИВИ ЄС. ЦИФРОВА ТА САМОСУВЕРЕННА ІДЕНТИЧНІСТЬ

Від тих рішень, які ми приймаємо сьогодні залежить наше завтра. Але що робити в тому випадку, коли «завтра» наступає занадто швидко? Наше сьогодення з суспільними відносинами, які поки важко регулювати і з новими суб'єктами у цих відносинах, які нам ще треба буде ідентифікувати. В цілому майбутнє стало викликом для людей , бізнесу та держав. Відповіді на ці та багато інших питань шукають на всіх рівнях : на національному, регіональному та світовому.

Надзвичайні темпи розвитку новітніх технологій та поступова « віртуалізація» між людиною - людиною, людиною- державою, державою - державою та ін. Дало завдання людству не допустити підміни понять та підміни ідентичності у цьому віртуальному світі.

ЄС взяло на себе почесну місію не регіональному , європейському, рівні очолити процес регулювання та впровадження цифрових інновацій у сфері застосування блокчейн технології та у сфері інтернету речей . ЄС зробила наступні ключові кроки на шляху до лідерства у використанні системи блокчейн та цифрової ідентичності :

- 23 липня 2014 р - за сприяння Європейської комісії було затверджено Регламент про електронну ідентифікацію та довірчі послуги;
- 10 квітня 2018 р - 29 країн підписало Декларацію «Про співпрацю в рамках Європейського блокчейн партнерства» як було визначено в тексті Декларації метою підписання країнами учасницями цієї Декларації було уникнути фрагментарного підходу до використання можливостей блокчейн технології , створення сумісними зусиллями відповідної інфраструктури та посилити довіру користувача цифровими послугами в межах Єдиного цифрового ринку.
- пізніше в квітні 2018 р в рамках альянсу European Blockchain Partnership було створено EBSI (European Blockchain Service Infrastructure) , яка являє собою однорангову мережу в якій ноди на європейському рівні регулюються Єврокомісією , а на національному рівні - країнами учасницями цієї ініціативи.

Для того щоб реалізувати довіру одне до одного суб'єктів, які здійснюють цифрові правочини , наприклад в рамках смарт контрактів цим суб'єктам треба чітко розуміти з ким вони мають справу. Тобто, ми торкаємось питання ідентичності. Якщо з ідентичністю у загальному розумінні все більш менше ясно, то дефініція «цифрова ідентичність» або “ самоуверенна ідентичність” (Self-Sovereign Identity (SSI)) є наразі не дуже поширеним в національному просторі. Тим не менш, в європейському правовому контексті цей термін вже сягнув своєї популярності.

Отже, цифрова ідентичність - це набір даних про особу, яку можна знайти у цифровому просторі і це та інформація, яка може нас ідентифікувати. Так як доволі часто можна почути про крадіжку персональних даних та витік персональної інформації можна зробити висновок, що досі не повною мірою реалізовані механізми інтероперабельності та цілісності захисту персональних даних та кібербезпеки на глобальному рівні.

Термін « самоуверенна ідентичність» або Self-Sovereign Identity (SSI) виник в рамках Регламенту eIDAS головна ідея цього терміну є те , що суб'єкт отримує можливість контролювати цифрові дані , цифрові активи, документи , сертифікати , тощо. SSI це певна модель реалізації цифрової ідентичності. Також, вона включає в себе можливість використовувати цифрові активи та передавати їх третій стороні у разі необхідності для доведення свого права власності , третій стороні не треба

звертатись до емітенту для їх перевірки так як це буде суперечити правилам використання технології блокчейн.

В рамках обраного і конституційно визначеного стратегічного європейського напрямку України і її майбутнього. Актуальність питання реалізації механізмів ідеї самосуверенної ідентичності є вкрай високим для уможливлення виходу громадян України в цифровий економічний та культурний простір, на всіх його рівнях: світовому, регіональному та національному.

Література:

1. Declaration on European Partnership on Blockchain 2018. URL: https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership (Last accessed: 29.04.2021

2. eIDAS Regulation (Regulation (EU) N°910/2014). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (Last accessed: 29.04.2021)

3. eIDAS Supported Self - Sovereign Identity . URL: https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf (Last accessed: 29.04.2021)

Іщенко А.А.

курсант ІСЗЗІ, КПІ ім. Ігоря Сікорського

Висоцький І.С.

курсант ІСЗЗІ, КПІ ім. Ігоря Сікорського

Науковий керівник: Кубайчук О.О.,

к.ф.-м.н., доцент, професор спеціальної кафедри №1, ІСЗЗІ

КПІ ім. Ігоря Сікорського

ПОГЛЯД НА ПРАВОВІ ОСОБЛИВОСТІ І ПРОБЛЕМИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ МЕДИЦИНИ

Цифрові технології поширюються серед людства, поглинаючи все більш важливі і відповідальні сфери людського життя. Навіть така давня наука як медицина не стала виключенням з правил. Проте все гостріше стає питання щодо правового регулювання штучного інтелекту саме у галузі медицини, бо саму тут вирішуються питання щодо здоров’я, життя та смерті живих істот.

Тому відповідальність за помилку вкрай висока - потрібно чітко провести межі того, хто буде винним.

Штучний інтелект в медицині є абсолютно новим словом, яке вимагає пильної уваги з боку не тільки інвесторів, лікарів і пацієнтів, а й законодавців. Дякуючи штучному інтелекту фахівці з охорони здоров'я можуть вирішувати надзвичайно складні і енергозатратні завдання. Штучний інтелект може виявитися цінним ресурсом для медичних працівників, допомагаючи їм в
повній мірі реалізувати свій досвід і потенціал.[1, с. 64]

Поки дана сфера ніяк не регламентується законодавством, але в майбутньому може серйозно впливати на роботу медичних закладів та установ. При цьому не варто забувати, що стовідсотково точні і достовірні результати машини показують далеко не завжди: є ймовірність виникнення помилок, тому так важливо, щоб була правова база, що в деталях регламентує особливості даної сфери.

Таким чином перед суспільством постають наступні завдання для їх вирішення шляхом створення законодавчої бази:

- накладення відповідальності за дії штучного інтелекту на фізичну особу, що створила штучний інтелект. Або ж, в якості альтернативи, покласти всю відповідальність на самого пацієнта, який має надавати згоду на лікування
за допомогою штучного інтелекту;

- чітке визначення особи, якій буде присвоєно право на інтелектуальну власність у випадку, якщо штучним інтелектом буде здійснюватися дослідницька робота(розробка медикаментів, пошук допустимих хімічних реакцій шляхом аналітичного підбору нових реагентів, біологічні симуляції, тощо);

- розробка та впровадження шаблонів взаємодії з штучним інтелектом та вирішення проблем з ліцензуванням медичних систем штучного інтелекту[2, с 43].

Однак не все так погано як може здатися на перший погляд: на даний момент вже робляться деякі кроки щодо правового впровадження штучного інтелекту у медичний простір. Сюди входять такі законодавчі акти, як Європейський загальний регламент про захист даних (GDPR) [3, с. 45]. GDPR відноситься до пацієнтів у межах ЄС та детально визначає вимоги щодо згоди на використання даних про пацієнтів. У травні 2016 року Білий дім оголосив про свій план проведення низки семінарів та формування підкомітету Національної ради з питань науки і технологій (NSTC) з питань машинного навчання та штучного інтелекту. У жовтні 2016 року рада опублікувала Національний стратегічний план досліджень та розвитку штучного інтелекту, в
якому окреслила запропоновані пріоритети досліджень та розробок штучного інтелекту.

Якщо говорити про Україну, то можна побачити значний прогрес по впровадженню штучного інтелекту у багатьох сферах. Зокрема, Міністерством та Комітетом цифрової трансформації була розроблена Концепція розвитку штучного інтелекту в Україні до 2030 року, де були поставлені основні пріоритетні сфери держави, які потребують впровадженню штучного інтелекту.

Дослідивши цей документ можна побачити, що медичний сегмент згадується у розділі «Публічне управління», де планується залучення штучного інтелекту у сфері охорони здоров'я, зокрема щодо протидії епідеміям та пандеміям, а також прогнозування та попередження потенційних епідемічних спалахів у майбутньому Відповідно, ставляться завдання, виконання яких повинні допомогти вирішити проблеми на законодавчому рівні, в тому числі й ті, що були згадані вище[4].

Отже, робота над впровадженням штучного інтелекту в людське життя триває. Нові рішення стосовно цієї теми активно обговорюються та приймаються. Не будуть зайвими і слова про те, що розробка законодавчої бази є майже такою ж важливою як і розробка самого штучного інтелекту.

Література:

1. Морхат П.М. К вопросу о специфике правового регулирования искусственного интеллекта и о некоторых правовых проблемах его применения в отдельных сферах // Закон и право. - 2018. - № 6. - URL: https://cyberleninka.ru/article/n/k-voprosu-o-spetsifike-pravovogo-regulirovaniya-iskusstvennogo-intellekta-i-o-nekotoryh-pravovyh-problemah-ego-primeneniya-v-otdelnyh (дата обращения: 05.11.2018)

2. Prakken H. On how AI & law can help autonomous systems obey the law: a position paper // AI4J — Artificial Intelligence for Justice. 2016. P. 42—46.

3. Lacassie E, Marquet P, Martin-Dupont S, Gaulier JM, Lachâtre G (September 2000). "A non-fatal case of intoxication with foxglove, documented by means of liquid chromatography-electrospray-mass spectrometry". Journal of Forensic Sciences.

4. Розпорядження Кабінету міністрів України «Про схвалення Концепції розвитку штучного інтелекту в Україні» від 2 грудня 2020 р. № 1556-р, URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

Kisil Anastasiya
1st year student Faculty of Sociology and Law
Igor Sikorsky Kyiv Polytechnic Institute
Supervisor: Inna BORKOVSKAYA,
Senior Lecturer of National Technical
University of Ukraine
Kyiv Polytechnic Igor Sikorsky Institute

LEGAL REGULATION OF CRYPTOCURRENCY CIRCULATION IN UKRAINE

Among a large number of digital resources and innovations, a special place in the development of each state is occupied by cryptocurrency. Every day more and more countries are choosing the strategy of legalization of e-currency, which has a positive impact on both the economic situation and their place in the international arena. Despite the rapid integration of cryptocurrency laws, the issue of legal consolidation in Ukraine remains open and orderly. Cryptocurrency is a digital currency, the unit of this currency is the "coin". Ukraine has not adopted regulations governing relations in the field of electronic currencies yet, so there is no direct ban on the purchase, possession or disposal of cryptocurrency, respectively, and there is no normative definition of this currency. However, it should be noted that there are bills aimed at legalizing and consolidating the legal regulation of cryptocurrency in our country, in particular the bill № 3637 "On Virtual Assets", which has been passed from the first reading. It directly relates to the legal relations arising in connection with the circulation of virtual assets in Ukraine, as well as identifies the rights and obligations of the participants in this circulation. The National Bank of Ukraine, which supports the bill, assessed this act, but notes that calling the currency a "crypt" is incorrect and impractical, due to its legal nature, which is more complicated than the concept of currency [Galushka, Pakon, 2017].

The bill № 2461 "On Amendments to the Tax Code of Ukraine and other laws relating to the taxation of transactions with cryptocurrencies, which specifies the terms "virtual asset", "cryptocurrency", "cryptocurrency transaction", "distributed register", "token" and "token-asset", which will help to avoid conflicts in the legislation regarding the interpretation of these expressions.

Another important document concerning the regulation of the cryptocurrency market is the Law of Ukraine "On Prevention and Counteraction to Legalization of

Proceeds from Crime, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction." In particular, the list of subjects of primary financial monitoring includes organizations whose activities are related to the accounting of electronic currency. Thus, if the company makes payments in cryptocurrency in the amount of more than 30 thousand UAH in equivalent, it is obliged to check this transaction and establish information about the client. The client, in turn, must provide complete information about the origin and destination of their virtual assets. If it is established that he received these funds illegally, it is not possible to stop the operation, but it is possible to block the cryptocurrency and seize illegally obtained cryptocurrencies.

After analyzing the regulatory framework and algorithm for legalization of cryptocurrencies, it should be noted that it is illogical. Because, the legislator makes changes first of all to the Tax code, at once solving a question of the taxation, however the question of interpretation of cryptocurrency remains open. Therefore, it is necessary to first amend the Civil Code, which should regulate all these legal relations. It should specify what a cryptocurrency is, what exactly can be done with these assets, what rights are granted to the user and what is the mechanism for their protection.

Examining the practical use of cryptocurrencies in Ukraine, we should pay attention to the Global Crypto Adoption Index, compiled by the American organization Chainalysis, in which our country ranks 1st in terms of cryptocurrency transactions. However, despite such statistics, Ukrainian companies that provide services for the exchange, storage, sale, transfer of electronic money are forced to work in the shadows, due to constant law enforcement and seizure of digital currency and equipment (under the pretext of combating terrorist financing, etc.) [Protsenko, 2016].

Legalization of cryptocurrencies in Ukraine is important because users and participants in the electronic assets market will be endowed with legal protection. Companies will be able to operate officially and be protected from abuse and fraud. In addition, the state budget will be replenished with significant revenues in the form of taxes from the activities of crypto companies.

References:

1. Galushka, E. A., Pakon, O. D. (2017). The essence of cryptocurrencies and prospects for their development. *Young scientist*,4, 634-637. [in Ukrainian].

2. Protsenko, A. T. (2016). Legal regulation of electronic money circulation in Ukraine. *Doctor's thesis*. Kiev: MAUP [in Ukrainian].

Корнійчук Наталія
Студентка, КПІ ім. Ігоря Сікорського

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ОБ'ЄКТ АВТОРСЬКОГО ПРАВА

Стрімкий науково-технічний прогрес (далі – НТП) диктує свої правила для всього людства, змушуючи пристосовувати загальносуспільні відносини, а разом з ними і нормативно правові акти під жвавий еволюційно-технологічний крок. Флагманом усього НТП є штучний інтелект (далі – ШІ), займаючи одночасно лідерство серед інновацій та гострих правових питань сьогодення.

Актуальність досліджуваної теми обумовлена необхідністю збагачення та тлумачення міжнародного правового досвіду у питаннях регулювання діяльності штучного інтелекту, як самостійної системи, рівною за своєю виробничою сутністю людині, зокрема в питанні інтелектуальної власності.

Загальноприйняте визначення окреслює ШІ інтелект досить сухо, адже було введено ще в 1956 році професором Дартмундського коледжу Джоном МакКарті [1,с. 126], що виділяв ШІ, як розділ комп`ютерної лінгвістики та інформатики, що формалізує завдання, які нагадують справи, що виконує людина.. На сьогоднішній день, технологія модельованого інтелекту вирвалася за кордони терміну, вирішуючи задачі без способів розв'язання, моделюючи вищу людську нервову діяльність, самонавчаючись, та звільняючи чималу кількість людей від рутинної роботи. Таким чином, ШІ запустив міцне коріння у теоретичну та практичну сферу науки, виробництва, творчості та підприємництва. Тому, тема штучного інтелекту широко обговорюється серед українських та закордонних правознавчих кіл, як актуальна та гостро денна.

Найбільш активними вітчизняними агітаторами розробки нормативно-правових актів стосовно діяльності ШІ є О. Єфічук (керівник практики права інтелектуальної власності ЮК Jurimex), С. Головко (юрист правової корпорації «Татаров, Фаринник, Головко»), Б. Дзяман (юрист ЮК Bossom Group), І. Городиський (кандидат юридичних наук, директор Школи права Українського католицького університету) та А. Афян (засновник юридичної компанії Juscutum).

Проблема авторського права на твори штучного інтелекту досить дискусійна, адже українське законодавство, згідно «Закону України про авторське право та суміжні права» [2] не регламентує порядку використання та право власності на твори, створені без участі людини, визначаючи правовласником твору виключно

фізичну особу. Отже, українське законодавство є застарілим відносно питань інтелектуальної власності, хоча й світова практика не втішна, більшість найпрогресивніших країн теж не спішить із розробкою законодавчих актів, які б утвердили робота, а той й віртуального бота як повноправного власника твору.

Це спричинено в більшій мірі різними точками зору на проблему, адже більшість науковців, а разом з ними і правознавців у сфері технологій визначають ШІ лише як гарний інструмент в руках програміста, на кшталт пера для письменника або пензля для митця. Дійсно, машинне навчання діє по закладеним у програму алгоритмам, використовуючи загальну базу даних (з англ.. Big Data), що дозволяє машині самостійно розробляти і приймати найбільш раціональні рішення, проте коли вони застосовуються до мистецтва, музики і літературних творів, алгоритми машинного навчання здійснюється лише на вході, на матеріалах наданих програмістом. Система автономно вивчає надані дані, створюючи нові частини роботи, приймаючи незалежних рішень протягом усього процесу, щоб визначити, як виглядає нова робота. Унікальністю такого типу ШІ є повністю генерований комп'ютерною програмою, так званою нейронною мережею, процес розумової діяльності подібної людській.

Українські вчені розділяють проблему встановлення правової діяльності людини перед своїм «віртуальним колегою», виділяючи кілька категорій творів: створені людиною та оброблені штучним інтелектом і самостійні (створені виключно роботом на основі проаналізованих творів мистецтва). Прикладом перших є обробка фотоматеріалів у редакторі Photoshop, в такому випадку автором визнається фізична особа, завдяки творчій праці якої було отримано кінцевий результат, що узгоджується з всесвітньою судовою практикою. Суд Європейського Союзу в одному із процесів зазначав, що авторське право поширюється тільки на роботи, оригінальність яких відображає власну інтелектуальну творчість автора. З другою категорією мистецьких творів усе набагато складніше, адже наразі більшість країн світу законодавчо не визнає штучний інтелект автором твору.

Та експерти передрікають різку зміну ситуації у найближчий час. Європарламент вже активно розробляє питання регуляції права ШІ на власно створенні твори, зокрема припускається можливість введення терміну «електронна особа» (electronic person). Першим кроком у цьому напрямку стала нещодавно прийнята Резолюція «Норми цивільного права про робототехніку» [3]. Документ, що складається з понад сотні пунктів, присвячений найрізноманітнішим аспектам і проблемам робототехніки та штучного інтелекту. Японське законодавство виявилося ще прогресивнішим і вже з 2016 року ведеться розробка та поступове впровадження нормативних документів, які б захистили авторське право на продукти творчої

діяльності, створені нейронними системами. Таке рішення має підтримати розвиток інноваційних компаній.

Тож, загально світова тенденція безперечно на стороні захисників прав роботів та інтелектуальних систем, але правове затвердження власності машини на свої твори буде сущою формальністю та популізмом, поки названий суб’єкт не матиме хоча б потенційної можливості на реалізацію цього права, хай навіть шляхом відмови від користування ним. Наразі, результатом автономної роботи ШІ є твори, які відповідають вимогам, що висуваються до винаходів чи витворів мистецтва, проте не існує програм, які були б здатні не просто видати творчий результат, а й, наприклад, свідомо заборонити його використання.

Законодавство нашої країни пов’язує створення обєктів штучним інтелектом і його авторство лише з людиною, через цю призму відповідно комп’ютери або ж певні комп’ютерні програми та інші форми вираженні ШІ не є винахідниками. Можливо така ситуація склалася через те що сам ШІ не розглядається як окремий суб’єкт.

Ні в Україні, ні в інших державах твори які були створені штучним інтелектом, не є об'єктами права інтелектуальної власності. Їх можна використовувати без обмежень. Однак така ситуація не буде тривалою, оскільки стрімкий розвиток потребує подальшого правового врегулювання і захисту прав відповідних суб'єктів. Ігнорування ж питання правової охорони об'єктів, створених штучним інтелектом, призведе до незацікавленості ринку в розвитку відповідних технологій у зв'язку з їх незахищеністю.

Отже, широка роботизація з використанням штучного інтелекту все глибше і глибше проникає в наше життя, змушуючи стагнуючі громадські науки не відставати від НТП, хоча ситуація з затвердженням авторського права по відношенню до ШІ в багатьох країнах світу, найближчим часом може стати прецедентом. Вперше, нормативно-правове регулювання буде орієнтиром, а не наздоганяючим в науковій сфері, надавши інтелектуальним системам по істині демократичне право розпорядження своїми напрацюваннями, як тільки вони досягнуть необхідного рівня розвитку, в чому, втім, сумніватися не доводиться.

Література:

1. Маккарти Джон. Большая советская энциклопедия: в 30 т. / за ред.: А. М. Прохоров — 3-тє вид., 1969. 800с.

2. Конституція України: Закон від 28 червня 1996 р. База данних «Законодавство України»/ВР України –URL:http://zakon3.rada.gov.ua/laws. (дата звернення 24.04.2021)

3. Резолюція Європарламенту від 16 лютого 2017 року 2015/2013(INL) P8_TA-PROV(2017)0051.– URL: http://robopravo.ru/riezoliutsiia_ies. (дата звернення 24.04.2021)

4. Олексій Кривецький. До проблеми правового регулювання штучного інтелекту. 01.24.2017 — URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=3728:do-problemi-pravovogo-regulyuvannya-shtuchnogo-intelektu&catid=8&Itemid=350 (дата звернення 24.04.2021)

5. Тамара Воліна. Складно бути роботом. 20.07.2018 — URL: https://zib.com.ua/ua/print/133716avtorom_tvoru_shtuchnogo_intelektu_mozhe_buti_viznana_lishe_.html (дата звернення 24.04.2021)

Ланкін Сергій

Студент, КПІ ім. Ігоря Сікорського
Науковий керівник: Дубняк М.В.,
к.ю.н., старший викладач
кафедри інформаційного права та
права інтелектуальної власності
КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ВИЗНАЧЕННЯ ПОНЯТТЯ ВІРТУАЛЬНИХ АКТИВІВ ТА СТАТУСУ КРИПТОВАЛЮТИ В УКРАЇНСЬКОМУ ЗАКОНОДАВСТВІ

Концепція віртуальних активів з розвитком технології та процесу цифровізації в 21 столітті для нашого суспільства вже не є предметом новітніх та ризикових досліджень та викликів. Різні види криптовалют економічно та фактично вже мають статус подібний або ідентичний до грошових коштів в їх цивільно-правовому та економічному розумінні. Незважаючи на те, що юридичний статус віртуальних активів ще врегульований досить загально, і як звично українському цивільному законодавству поки що регулюється за аналогією, навіть народні депутати України вже почали вказувати критовалюту у власних деклараціях про доходи, зокрема такі види криптовалюти як Bitcoin та Etherium, NXT, Ripple та Litecoin.[2]

Хоча держави навіть передових країн світу все ще досить побічно та на власний ризик інтегрують криптовалюти у власний цивільний обіг та економіку, деякі приватні компанії, що підтримують такого роду реформації вже цілком легально дозволили проводити оплати за допомогою криптовалюти, як це робить Ілон Маск та його компанія з виробництва автомобілів майбутнього Tesla, що не могло не відкликнутись на курсі основної критовалюти світу Bitcoin.[7]

Неврегульованість законодавчо статусу криптовалюти зумовлена вочевидь слабким розумінням державними фінансовими інститутами та державними діячами загалом її принципів діяльності та існування, а відтак чого не можеш зрозуміти за змістом не можливо й правильно розтлумачити.

Логічним наслідком такої проблеми є подання чисельних законодавчих ініціатив народними депутатами України до Верховної Ради України, які де інде зберігають послідовність регулювання та принципових положень, але загалом думки з приводу правового статусу віртуальних активів в Україні у законодавця різні.

До прикладу можна взяти визначення криптовалюти надане в Законопроекті №7183 від 06.10.2017, який був покликаний врегулювати обіг криптовалюти в Україні.[5]

Зокрема основним ознаками, які виділяються в законопроекті у визначенні криптовалюти є те, що вона є програмним кодом і дані про нього зберігаються в системі блокчейн у формі такого же програмного коду, також, що криптовалюта є об'єктом права власності та не є засобом міни.

Відтак зважаючи на те, що таке визначення є одним з найпершим намагань легалізувати статус віртуального активу в Україні, для першого законопроекту ці напрацювання мали свій сенс та вклад в розвиток законодавчого процесу визначення статусу криптовалюти в Україні, але така дефініція не витримала жодної критики від Головного наукового-експертного управління, та загалом від юридичної спільноти, яка має хоч загальне розуміння принципів діяльності криптовалюти.

Відтак намагання визначити економічний зміст криптовалюти були через пряме зазначення про те, що вона є об’єктом права власності. Напевне для законодавця це було певною поміткою для того, щоб відрізнити криптовалюту від просто набору програмного коду, але такий висновок не є досить доречним, про що зазначили експерти, адже будь-яка річ, якою особа володіє, може користуватись та розпорядитись без жодних перешкод її долею, вже є по суті правом власності на нею, і окремої легалізації не потребує.

Іншим цікавим положенням є пряма заборона укладання договору міни щодо криптовалюти (адже вона не може бути засобом міни), що знову ж таки обмежує по суті розпорядження майном власника у вигляді криптовалюти, підстави для цього нажаль логічно або напряму законодавцем не пояснюються.

Саме тому на даний момент даний законопроект відкликаний, оскільки як ми вже з’ясували має суттєві недоліки.

Іншим намаганням про стимулювати розвиток криптовалюти в Україні був Законопроект №7183-1 від 10.10.2017, де під криптовалютою вже розумівся

децентралізований цифровий вимір вартості, який є засобом обміну, збереження вартості, або одиницею обліку, яка заснована на математичних обчисленнях і вважається фінансовим активом.[6]

Одним з найперших та досить змістовних зауважень науково-експертного управління для даного визначення є те, що створювати окремий закон саме для фінансового активу, на якому наполягає законодавець не досить доцільно, оскільки законодавство України вже має досить розвинути базу про фінансові активи, і доцільніше було б внести зміни до вже існуючого законодавчого масиву для уникнення елементарного законодавчого спаму.

З іншого боку позитивним є намагання законодавця визначити не лише форму а й певний зміст криптовалюти, яка по суті є виміром вартості та засобом обміну, який генерується за допомогою обчислень, тому порівняно з іншим законопроектом в даному випадку помітний величезний прогрес технічного розуміння функціонування криптовалюти, що каже про реальні перспективи впровадження такої ініціативи в чинне українське законодавство.

Відтак підводячи підсумки можна сказати на те, що напряму поняттям «криптовалюта» на сьогодні законодавство України не оперує, і єдине, що ми маємо в чинному масиві законодавства, це визначення віртуального активу надане в п. 13 ст. 1 Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».[1]

А саме: віртуальний актив – цифрове вираження вартості, яким можна торгувати у цифровому форматі або переказувати і яке може використовуватися для платіжних або інвестиційних цілей;

Як бачимо суттєво від визначення зазначеного в законопроекті (№7183-1 від 10.10.2017) немає, фундаментальним залишилось розуміння вираження цифрової вартості та цілей криптовалюти. Звісно, станом на сьогодні не можна сказати, що одне визначення замінить цілий пласт фінансових відносин в суспільстві, але станом на сьогодні є хоча б підстави думати про можливий розвиток законодавства в цьому напрямку в майбутньому.

Якщо дивитись на вираження криптовалюти саме в формі віртуального активу, то такі визначення надавались в Законопроектах пов’язаних з віртуальними активами №3637 від 11.06.2020 та №2461 від 15.11.2019, де під ними зокрема розумілась цифрова форма майна, операції з якою відбуваються електронно. Вводиться також поняття токен-актив, який обраховується в певному реєстрі і може існувати в системі обігу віртуальних активів.[4][3]

Відтак найцікавішим моментом даного законопроекту була б його практична реалізація, а саме яким чином законодавець збирався створювати такий реєстр, та яка кількість осіб дійсно мала б бажання легально ідентифікувати власні активи для їх теоретичного оподаткування.

Таким чином станом на сьогодні в правовій системі Україні ще не вирішено досить багато питань, що стосуються статусу криптовалюти, її економічного та юридичного змісту, режиму оподаткування та обліку, а також правовий режим передання та чи потрібна її державна реєстрація, хоча вищезазначені законопроекти дають велику надію на майбутню легалізацію такого предмету товарно-грошових відносин в суспільстві.

Література:

1.Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення». Відомості Верховної Ради України. 2020. URL: https://zakon.rada.gov.ua/laws/show/361-20#n831 (дата звернення 20.04.2021).

2.Близько 15 народних депутатів задекларували заощадження у криптовалюті. Радіо Свобода. 2021. URL: https://www.radiosvoboda.org/a/news-deputaty-kryptovalyuta/31188083.html (дата звернення 20.04.2021).

3.Проект Закону про віртуальні активи № 3637 від 11.06.2020. Верховна Рада України. 2020. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110 (дата звернення 20.04.2021).

4.Проект Закону про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами № 2461 від 15.11.2019 Верховна Рада України. 2019. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67423 (дата звернення 20.04.2021).

5.Проект Закону про обіг криптовалюти в Україні № 7183 від 06.10.2017. Верховна Рада України. 2017. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684 (дата звернення 20.04.2021).

6.Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні № 7183-1 від 10.10.2017. Верховна Рада України. 2017. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710 (дата звернення 20.04.2021).

7.Tesla дозволила купляти електромобілі за біткоїни: курс криптовалюти відразу різко зріс. AutoGeek. 2021. URL: https://autogeek.com.ua/tesla-dozvolyla-kupliaty-elektromobili-za-bitkoiny-kurs-kryptovaliuty-vidrazu-rizko-zris/ (дата звернення 20.04.2021).

Лаушкін Ілля

Студент, КПІ ім. Ігоря Сікорського

ПРАВОВІ АСПЕКТИ ТА ПРОБЛЕМИ НОРМАТИВНОГО РЕГУЛЮВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ

Науково-технічний прогрес зумовив широке впровадження інформаційних технологій в усіх галузях життєдіяльності суспільства. Роль інформаційних технологій полягає в підвищенні рівня ефективності виробництва, прибутку, конкурентоспроможності тощо не тільки за рахунок збільшення продуктивності праці, підвищення якості та швидкості прийняття управлінських рішень, але й за рахунок організації нових способів роботи з клієнтами і постачальниками.

Для розвитку інформаційного суспільства стало характерним поєднання глобальних інформаційно-комунікаційних систем, інтеграція баз даних та знань, зростання спектру послуг і сервісів, різке збільшення клієнтського навантаження на серверний простір. А результатом цього еволюційного руху став розвиток інформаційних технологій, а саме поява та розвиток «хмарних технологій». Щодо визначення понять, то необхідно звернутися до провідних наукових установ Європейського союзу та США.

У 2012 році Європейська комісія прийняла стратегію «Розкриття потенціалу хмарних обчислень в Європі» і саме в цій стратегії розкривається поняття хмарних технологій та обчислень. «Хмарні обчислення — зберігання, обробка та використання даних на дистанційно розташованих комп’ютерах шляхом отримання доступу через Інтернет»[1].

Дослідження щодо розвитку та вдосконалення хмарних технологій проводить Національний Інститут стандартів та технологій США. Саме цей інститут і надає таке визначення: «Хмарні обчислення — модель надання широкого і зручного мережевого доступу до загального пулу керованих обчислювальних ресурсів та їх послуг, які можуть бути швидко надані або звільнені з мінімальними зусиллями з системи управління при необхідності забезпечення взаємодії з провайдером послуг» [2].

Щодо розрізнення хмарних технологій, то в суспільстві існує декілька моделей їх розрізнення:

1. За моделлю розгортання розрізняють:

- “Приватна хмара” (англ. – private cloud) – інфраструктура, призначена для використання однією організацією, що включає кілька споживачів (наприклад,

підрозділів однієї організації), можливо також клієнтами і підрядниками даної організації. Приватна хмара може перебувати у власності, управлінні та експлуатації як самої організації, так і третьої сторони (або будь-якої їх комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника.

- “Публічна хмара” (англ. – public cloud) – інфраструктура, призначена для вільного використання широкою публікою. Публічна хмара може перебувати у власності, управлінні та експлуатації комерційних, наукових та урядових організацій (або будь-якої їх комбінації). Публічна хмара фізично існує в юрисдикції власника постачальника послуг.
- “Суспільна хмара” (англ. – community cloud) – вид інфраструктури, призначений для використання конкретною спільнотою споживачів з організацій, що мають спільні завдання (наприклад, місій, вимоги безпеки, політики та відповідності іншим різним вимогам). Суспільна хмара може перебувати в кооперативній (сумісній) власності, управлінні та експлуатації однієї або більше з організацій співтовариства або третьої сторони (або будь-якої їх комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника.
- “Гібридна хмара” (англ. – hybrid cloud) – це комбінація з двох або більше різних хмарних інфраструктур (приватних, публічних або суспільних), що залишаються унікальними об’єктами, але пов’язані між собою стандартизованими чи приватними технологіями передачі даних і додатків (наприклад, короткочасне використання ресурсів публічних хмар для балансування навантаження між хмарами) [3].

2. За моделями обслуговування:

- Програмне забезпечення як послуга (SaaS, Software as a Servise) – споживачеві надаються програмні засоби – додатки провайдера, що виконуються на хмарній інфраструктурі.
- Платформа як послуга (PaaS, Platform as a Service) – споживачеві надаються засоби для розгортання на хмарній інфраструктурі створюваних споживачем або придбаних додатків, що розробляються з використанням підтримуваних провайдером інструментів і мов програмування.
- Інфраструктура як послуга (IaaS, Infrastructure as a Service) – споживачеві надаються засоби обробки даних, зберігання, мереж та інших базових обчислювальних ресурсів, на яких споживач може розгортати і виконувати довільне програмне забезпечення, включаючи операційні системи та програми [4]

Щодо національного законодавства, нормативного закріплення основ та термінів хмарних технологій, то тут необхідно звернутися до проекту закону «Про хмарні послуги», в якому надається декілька визначень, які стосуються хмарних технологій та, на мою думку, в певній мірі розкривають суть хмарних технологій:

- технологія хмарних обчислень – технологія забезпечення дистанційного доступу на вимогу до хмарної інфраструктури через електронні комунікаційні мережі;
- хмара (хмарна інфраструктура) – це сукупність динамічно розподілюваних та налаштовуваних хмарних ресурсів, які можуть бути оперативно надані користувачу хмарних послуг і вивільнені через глобальну та локальні мережі передачі даних;
- хмарні ресурси - будь-які технічні та програмні засоби або інші компоненти інформаційної (автоматизованої) системи, які доступні за допомогою технології хмарних обчислень, такі як процесорний час (обчислювальна потужність), місце в сховищах даних, обчислювальні мережі, бази даних і комп’ютерні програми. [5]

Проаналізувавши проект Закону України «Про хмарні послуги» та інформацію з сайту «ВалТек», то ми можемо побачити, що в проекті надаються терміни щодо хмарної інфраструктури, а саме:

Проект Закону	**Інформація з інтернет-ресурсу**
Приватна хмара - хмарна інфраструктура, що підготовлена для використання єдиним користувачем хмарних послуг та контролюється ним.	“Приватна хмара”– інфраструктура, призначена для використання однією організацією, що включає кілька споживачів (наприклад, підрозділів однієї організації), можливо також клієнтами і підрядниками даної організації. Приватна хмара може перебувати у власності, управлінні та експлуатації як самої організації, так і третьої сторони (або будь-якої їх комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника.
Колективна хмара - хмарна інфраструктура, що поділена між особливою групою	“Суспільна хмара”– вид інфраструктури, призначений для використання конкретною спільнотою

взаємопов’язаних користувачів хмарних послуг, які мають спільні потреби, та що контролюється представником або представниками цієї групи.	споживачів з організацій, що мають спільні завдання (наприклад, місій, вимоги безпеки, політики та відповідності іншим різним вимогам). Суспільна хмара може перебувати в кооперативній (сумісній) власності, управлінні та експлуатації однієї або більше з організацій співтовариства або третьої сторони (або будь-якої їх комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника.
Публічна хмара - хмарна інфраструктура, що потенційно доступна для невизначеного кола користувачів хмарних послуг та контролюється надавачем хмарних послуг.	“Публічна хмара”– інфраструктура, призначена для вільного використання широкою публікою. Публічна хмара може перебувати у власності, управлінні та експлуатації комерційних, наукових та урядових організацій (або будьякої їх комбінації). Публічна хмара фізично існує в юрисдикції власника постачальника послуг.
Гібридна хмара - хмарна інфраструктура, що є композицією з двох або більше різних хмарних інфраструктур (приватні, колективні або публічні), що є самостійними об'єктами, пов'язаними між собою технологіями, що дозволяють переносити дані або комп’ютерні програми між цими об’єктами. [5]	“Гібридна хмара”– це комбінація з двох або більше різних хмарних інфраструктур (приватних, публічних або суспільних), що залишаються унікальними об’єктами, але пов’язані між собою стандартизованими чи приватними технологіями передачі даних і додатків (наприклад, короткочасне використання ресурсів публічних хмар для балансування навантаження між хмарами) [4]

Тож, порівнявши терміни, ми можемо зробити висновок, що законодавче закріплення термінів, їхні функції та сутність є менш розкритим ніж інформація з інтернет-ресурсів, що є проблемою та може призвести до виникнення певних питань стосовно правового визначення термінів та взагалі рулювання хмарних технологій. А отже ми можемо зробити висновок, що нормативне регулювання хмарних технологій, їх термінологія в законодавстві є такою, що потребує розвинення та вдосконалення. На мою думку, це можливо зробити за допомогою запозичення досвіду європейських країн-партнерів України, а також більш швидкого розгляду питання щодо прийняття змін до проекту закону та його прийняття.

Література:

1. Kroes Neelie. Towards a European Cloud Computing Strategy / NeelieKroes. URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/5
2. NIST SP 500-292 NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards and Technology. U.S. 2011.URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf
3. Сергей Глазунов. Бизнес в облаках. Чем полезны облачные технологии для предпринимателя. URL: www.kontur.ru/articles/225
4. Хмарні технології. Переваги і недоліки. URL: https://valtek.com.ua/ua/system-integration/it-infrastructure/clouds/cloud-technologies
5. Проект Закону України «Про хмарні послуги» // База даних «Законодавство України»/ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=2655&skl=10

Луценко А. С.

Студентка, КПІ ім. Ігоря Сікорського

ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВІЗАЦІЇ В АГРАРНІЙ ПРОМИСЛОВОСТІ

Процеси оцифровування є сучасним драйвером розвитку не лише економіки та суспільства, але і держави, що потребує комплексного впровадження цифрових трансформацій. На підтвердження цього є створення у вересні 2019 року Міністерства цифрової трансформації України [1] як головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері цифровізації, цифрового розвитку, цифрової економіки,

цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікаційних мереж, електронної комерції та бізнесу і т. д.

Із переліку основних завдань нового міністерства виділили напрями роботи пов'язані із сферою цифровізації економіки, в тому числі і сільського господарства. А тому актуалізація питань цифровізації аграрної промисловості потребує нагальної розробки дієвих механізмів і засобів практичного використання цифрових інновацій суб'єктами господарювання.

Однак чи варто впроваджувати цифрові ідеї у сферу агропромисловості? Україна має у своєму розпорядження 30 відсотків всього світового чорнозему та близько 60 відсотків від загальної площі держави, а тому логічним є те, що все пов’язане із сільськогосподарською галуззю – має великий потенціал. З огляду на її специфіку треба сказати, що навіть визнаючи необхідність діджиталізації варто розуміти, що така процедура в агропромисловості матиме свої особливості.

Цифрова трансформація агропромислового виробництва розглядається як один із основних шляхів зміни національної економіки, її переорієнтації з сировинної моделі експорту на постачання продуктів із високою доданою вартістю. Зниження витрат на виробництво аграрної продукції, підвищення її якості та конкурентоспроможності на основі ефективного використання ресурсів і науково обґрунтованих підходів – це головне завдання цифровізації сільського господарства [2, с. 127]

Головна мета їх розвитку полягає в тому, щоб усі громадяни України без обмежень та труднощів технічного, організаційного та фінансового характеру (зокрема соціально незахищені верстви населення) могли скористатися цифровими можливостями незалежно від свого місцезнаходження чи проживання та не перебували в сегменті «цифрового розриву» [3].

Однак в країні існують великі проблеми у впровадженні і поширенні цифрових технологій в підприємництві, виробництві та суспільному житті. Сьогодні більше 1/3 сільського населення України не мають доступу до широкосмугового Інтернету. Половина українських шкіл та майже всі заклади охорони здоров’я не підключені до всесвітньої мережі. Виправити цю ситуацію можливо: за допомогою проектів державно-приватного партнерства за кілька років досягти покриття широкосмугового Інтернету понад 80% [4].

Особлива увага щодо широкосмугового доступу до Інтернету повинна приділятися сільським територіям, що в свою чергу дозволить подолати цифровий розрив. Цифровізація сіл також підтримає розвиток сільського господарства, створить робочі місця, зменшить міграцію сільських мешканців до міст.

Насамперед, прикладами цифровізації здійснення інфраструктурного обслуговування є започаткування електронного фермерського реєстру, пілотний проект якого створювався на підставі Указу Президента України № 837/2019 від 08.11.2019 [5] метою якого є запровадження державної підтримки щодо підвищення фінансової спроможності фермерів та сільськогосподарських виробників. В наступному розширено коло учасників такого реєстру до всіх виробників сільськогосподарської продукції [6].

Наступним кроком є законодавче врегулювання функціонування Державного аграрного реєстру, для чого розроблено та внесено на розгляд Верховної Ради України законопроект № 3295 [7]. Законопроект спрямований на обов'язкову взаємодію усіх електронних реєстрів. Також, законопроект передбачає відповідні зміни в Законі України «Про державну підтримку сільського господарства України» [8]. Такі дії повинні кваліфікуватися як звичайний засіб господарсько – правового регулювання певних відносин фермера з суб'єктами та учасниками аграрного ринку.

Отже, використання сучасних технологій — це лише частина великого комплексу даних, які можливо отримувати за допомогою існуючих цифрових інструментів, проблема криється у правильній обробці і застосуванні наявної інформації. На жаль, поки що більшість сільськогосподарських підприємств використовує цифрові технології частково, а не повністю, що значно знижує загальний позитивний ефект від їх використання.

Цифровізація як напрям сучасної трансформації сільськогосподарських підприємств потребує глибинного переосмислення в напрямі пошуку можливостей застосування окремих складових технологій в залежності від напряму роботи підприємства.

Повноцінне впровадження децентралізації та прийняття відповідних цільових державних програм підтримки суттєво пришвидшить процес впровадження цифровізації в агросектор.

Література:

1. Питання Міністерства цифрової трансформації. — URL: https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919 (дата звернення: 25.04.2021)

2. Руденко М. В. Вплив цифровізації на розвиток агросфери. Матеріали міжнародної науково-практичної конференції. 2019. С. 127–129.

3. Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020). Концептуальні засади (версія 1.0). Першочергові сфери, ініціативи, проекти «цифровізації» України до 2020 року. HITECH office. – грудень 2016. – 90 с. URL : https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf

4. Державна служба статистики України. - URL : http://www.ukrstat.gov.ua/ (дата звернення: 25.04.2021)

5. Указ Президента України № 837/2019 від 08.11.2019. URL: https://www.president.gov.ua/documents/8372019-30389 (дата звернення: 25.04.2021)

6. Офіційний Веб-сайт Міністерства розвитку економіки, торгівлі та сільського господарства України. URL: https://www.me.gov.ua/?lang=uk-UA (дата звернення: 25.04.2021)

7. Нормативно-правове регулювання проведення пілотного проекту зі створення та функціонування державного аграрного реєстру. URL: http://valky-rda.kh.gov.ua/news/208/78502 (дата звернення: 25.04.2021)

8. Законопроект № 3295 від 30.03.2019. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68504 (дата звернення: 25.04.2021)

Diana Mazur

Student of faculty of Linguistics of
Igor Sikorsky Kyiv Polytechnic Institut
Supervisor: Olga Golovko,
PhD in Law, Senior Lecturer,
Department of Public Law
Igor Sikorsky Kyiv Polytechnic Institute

PROBLEM OF INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS DURING THE COVID-19 PANDEMIC

The XXI century is indeed a time of intellectual property because every day we can witness the birth of different goods made of human ideas for various directions of usage. In Ukraine, there are many problematic issues of legal regulations relating to this sphere. In particular, the unwillingness of society to respect the right of intellectual property, its disregard, as well as the lack of effective mechanisms for its defense from the side of the government are the main reasons for the growth of the counterfeiting products phenomenon [1, p. 300].

The need for effective legal protection of intellectual property rights and reduction of product falsification is a topical problem today as with the outbreak of the Covid-19 these issues have started to rapidly gain momentum at a national level. The lockdown

implemented by the government caused a severe economic recession, resulting in a dramatic growth of counterfeited goods manufacturing. The urgency of buying vital necessities such as medicines, food and hygienical products via the Internet has created perfect conditions for illicit business owners to retail counterfeit goods cheaper and gain enormous profits. Thus criminals make money by selling
counterfeit tests, drugs, disinfectants of unknown origin and a low quality that may be a deadly threat to humans' health and safety [2]. That is why it is essential to discuss such topics as consumer safety and Intellectual Property Rights protection of
legitimate businesses.

According to the “2020 Special 301 Report” Ukraine is again among the most pirated countries in the world. For such a long time, the work of Ukraine’s Collective Management Organization (CMO), which is in charge of keeping track of realisation of Intellectual property rights and dispensing royalties to right holders, has been non-transparent and unfair [3, p. 58]. Although our country established legislation that changed the CMO system in 2018, there is still plenty of work to do. Namely, to improve realisation of the results of intellectual creativity and innovation, which is the basis of a competitive economy of the country [4, p. 31]. Frequently, the Ukrainian government does not implement effectual measures to fight fast-spreading online infringement or so to say, the legislation does not keep up with the pace of world development and new inventions.

The enactment of increasing the responsibility for the infringement of intellectual property rights would reduce counterfeiting of original products which help to overcome the Covid-19 pandemic. Namely, generalization of investigative practice on crimes related to infringement of intellectual property rights, and unification of judicial practice in crimes of this category, which would ensure the unity of law enforcement [2]. In addition, amendments to the sanction of Art. 51-2 of the Code of Administrative Offenses, which entails the increase of the penalty and
confiscation of counterfeit products, equipment/raw materials used for production, would be a great step [2].

We assume that these amendments to the law are of significant importance for Ukraine, as counterfeiting not only reduces the profit of the state budget but either affects the consumers and may be a danger for their health. Ukraine is the country, sphere of intellectual property law of which should be improved and developed. Both government and certified brand owners should implement actions towards public awareness about the rapid rise in counterfeited commodities and ways to differentiate the authentic product from its imitation. By this is meant, that it is necessary to form a basic knowledge of intellectual property as a significant component of the legal culture of the population, that is why the related problem needs to be studied more in detail in the future.

Proper protection of Intellectual Property Rights is a key for economic growth which stimulates innovation development within the country. It means a significant importance to create the legal framework as an important condition for defending Intellectual Property Rights during the Covid-19 pandemic.

References:

1. Бошицький Ю. Л. Поглиблення правової культури громадян Як засіб оптимізації охорони інтелектуальної власності в Україні / Часопис Київського університету права. – 2020. – С. 300–305.
2. Пахаренко О. Кримінальний проступок, коронавірус та захист прав інтелектуальної власності / Олександр Пахаренко. // Юридична газета online. – 2020.
3. E. LIGHTHIZER R. 2020 Special 301 Report [Електронний ресурс] / ROBERT E. LIGHTHIZER. – 2020. – URL: https://data.consilium.europa.eu/doc/document/ST-15330-2019-INIT/en/pdf. (дата звернення 22.04.2021)
4. Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director. COMMISSION STAFF WORKING DOCUMENT Report on the protection and enforcement of intellectual property rights in third countries / Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director. – Brussels, 2019. – 58 c.

Мінькіна Дар`я

Студентка, КПІ ім. Ігоря Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ З ПОЗИЦІЙ ЦИВІЛЬНОГО ЗАКОНОДАВСТВА

Актуальність теми дослідження полягає у тому, що на даний момент існує велика кількість питань, яким необхідне краще правове регулювання щодо правового режиму штучного інтелекту. Дана ситуація виникла через невпинний розвиток інформаційних технологій та постійного розширення сфер, у яких використовується штучний інтелект.

У цивільному праві питання щодо врегулювання штучного інтелекту стоїть досить гостро, оскільки зараз його використовують як для створення нових об`єктів права інтелектуальної власності, так і у повсякденному житті.

У разі, якщо дані об`єкти не будуть віднесені до права інтелектуальної власності, то вони не будуть підпадати під охорону права власності. Також

важливим є питання визнання автором робіт, створених штучним інтелектом, і якщо так, то чи буде штучний інтелект суб’єктом права.

Законодавством України достатньо не врегульовано питання правового регулювання штучного інтелекту. На нашу думку, в подальшому необхідно удосконалити розвиток даного питання, оскільки штучний інтелект створений з метою полегшення та покращення подальшого життя суспільства.

На даний момент не існує єдиного підходу до визначення поняття штучного інтелекту та формування його визначення. Існує подібне визначення, що не входить до законодавства – «здатність побудови моделі поведінки на основі алгоритму вирішення завдань, сформованого свідомістю; це загальна здатність до пізнання і вирішення проблем, яка об’єднує всі пізнавальні здібності, такі як відчуття, сприйняття, пам’ять, уявлення, мислення, уява» (А. Азімов).

Так О. А. Баранов запропонував такі види штучного інтелекту та їх розуміння: – «Прикладний штучний інтелект» («слабкий штучний інтелект», «вузький штучний інтелект» або «обмежений штучний інтелект») розуміється, як сукупність комп’ютерних програм, які максимально наближено імітують одну або кілька когнітивних функцій і використовуються в процесі здійснення конкретної діяльності без участі людини для досягнення поставлених цілей відповідно до заздалегідь визначених критеріїв і параметрів.

Основними ознаками штучного інтелекту є динамічність, гнучкість, здатність до безперервного розвитку, можливість розуміти та розпізнавати інформацію та приймати рішення. На даний момент, штучний інтелект використовується у низці сфер, таких як медицина, спорт, банківська справа та інші. Саме тому існує нагальна необхідність удосконалення правового регулювання штучного інтелекту, оскільки без цього він так і залишиться без достатнього правового регулювання та охорони з боку держави.[1]

По-перше, необхідно визначити правосуб`єктність штучного інтелекту, оскільки без цього він не зможе увійти до цивільних правовідносин. Необхідно, щоб штучний інтелект був повністю незалежним, а для цього необхідний розгляд штучного інтелекту не як програми, винаходу або штучної моделі, від якої розробник може отримувати прибуток. [2] З цього випливає, що штучний інтелект має володіти тими ж правами та обов`язками, якими володіє людина, але при цьому мати певні особливості правового статусу порівняно з нею. На даний момент штучний інтелект розглядається лише як об`єкт цивільних прав. Більше того, цивільно-правова відповідальність дає підстави розуміти штучний інтелект як продукт (товар).

З огляду на все вищеописане, на нашу думку штучний інтелект відрізняється від усіх інших суб`єктів та об`єктів цивільного права, а тому існує необхідність подальшого удосконалення правового регулювання разі появи у штучного інтелекта волі та самостійного інтелекту.

Малайзійські вчені Hartini Saripan, Nurus Sakinatul Fikriah Mohd Shith Putera, Sheela A/P Jayabala з Університету технологій МАРА та науковець із США – Willick S. зазначили та наполягали на тому, щоб визнати штучний інтелект подібним до юридичної особи, зокрема: якщо казати про кінцеву мету щодо покладання відповідальності за дії роботів та штучного інтелекту, то може йтися про надання «розумним» роботам конституційних прав, та слід вважати їх юридичною особою.

Таким чином, можна припустити, що скоро у цивільному законодавстві з`явиться новий суб`єкт цивільних правовідносин, подібний по правовому статусу до юридичної особи.

Є.О. Харитонов та О.І. Харитонова також розглядають штучний інтелект як один із видів юридичної особи, науковці пропонують додати до видів правосуб’єктності юридичної особи таке положення як «кіберздатність», тобто здатність бути активним учасником відносин у ІТ-сфері [3].

Натомість, О.А. Баранов зазначає необхідність визнання роботів зі штучним інтелектом суб’єктами суспільних відносин, тому що «розумні роботи», які здійснюють людиноподібні дії в процесі відносин у взаємодії з традиційними суб’єктами повинні розглядатися як повноцінні суб’єкти цивільного права, які є на рівні з фізичними особами [4].

Підводячи підсумки, можемо визначити, що на даний момент питання визначення та правового регулювання штучного інтелекту з позицій цивільного законодавства все ж залишається відкритим. Єдиної думки щодо подальшого удосконалення регулювання цього питання з правової точки зору не існує. На даний момент, штучний інтелект залишається об`єктом права, оскільки є неживим та позбавленим будь-якої чутливості.

Питання визначення роботів зі штучним інтелектом як суб’єкта цивільного права залишається актуальним і недостатньо дослідженим, а тому ще довгий час будуть виникати прогалини і колізії у сучасній юриспруденції. Для того, щоб цього уникнути, потрібно прийняти низку законодавчих актів, які б дозволили будувати нову правову систему з новим суб’єктом права.

Література:

1. Мойсюк О.В. Право інтелектуальної власності на об’єкти, створені штучним інтелектом. 2020. URL: http://ekmair. ukma.edu. ua/ bitstream/

handle/123456789/18665/Moisiuk_Pravo_intelektualnoi_vlasnosti_na_obiekty,_stvoreni_shtuchnym_intelektom.pdf?sequence=5

2. Кошелєва К.О. Проблема надання правосуб'єктності штучному інтелекту. Юридичний бюлетень. Вип. 11. Ч. 1. 2019. URL: http://lawbulletin.oduvs.od.ua/archive/2019/11/part _1/9.pdf

3. Бежевець А.М. Правовий статус роботів: проблеми та перспективи визначення. Інформація і право. 2019. № 1(28). С. 61-67. URL: http://ippi.org.ua/sites/default/files/9_11.pdf

4. Баранов О.А. Ідентифікація робота з штучним інтелектом як суб'єкта права. Інтернет речей: проблеми правового регулювання та впровадження: матеріали наук.-практ. конф. (Київ, 29 лист. 2018 р.). Київ: Вид-во «Політехніка», 2018. С. 8-12

Ніжнік Владислав

Студент, КПІ ім. Ігоря Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЗАКОНОДАВСТВІ УКРАЇНИ ТА КРАЇН ЄВРОПЕЙСЬКОГО СОЮЗУ

Персональні дані займають провідне місце у нашому житті. Ми даємо згоду на обробку наших персональних даних майже у всіх сферах життя, крім випадків, які відносяться до національної безпеки, економічного добробуту та прав людини. [1] Тобто, спектр застосування «приватних» даних є дуже широким. І тому для того аби бути «підкованим» у сфері персональних даних і не втрапити на «гачок» до шахраїв необхідно звернутися до законів та міжнародних актів, які були ратифіковані Україною та порівняти їх зміст із законодавством країн Європейського Союзу. Актуальність дослідження даної теми обумовлена популярністю процедури обробки персональних даних.

Метою дослідження є поінформування громадян у сферу нормативного регулювання персональних даних та їх захисту в Україні та країнах Європейського Союзу, а також виділення проблеми безальтернативності згоди на обробку персональних даних.

В Україні питання захисту персональних даних регулюється Законом України «Про захист персональних даних». Повноваження на захист персональних даних належать Уповноваженому Верховної Ради України з прав людини.

Відповідно до Закону України «Про захист персональних даних» персональними даними вважаються відомості або сукупність відомостей про

фізичну особу, яка ідентифікована або може бути ідентифікована. [2] Такими відомостями є повне ім’я, псевдонім, дата народження, місце народження, вік, стать, сімейний стан, диплом про освіту, тощо.

Згідно до того ж Закону України обробкою персональних даних вважається будь-яка дія або сукупність дій із збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання і поширення (розповсюдження, реалізації, передачі), знеособлення, тобто вилучення, та знищення персональних даних. [2]

В статті 32 Конституції України зазначено, що не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. [1]

Опитавши своїх знайомих, я прийшов до висновку, що багато із них плутають поняття володільця і розпорядника персональних даних, тому, ми вирішили пояснити в чому між ними різниця із посиланням на закон.

Відповідно до статті 2 вже відомого нам Закону України «Про захист персональних даних» володілець персональних даних фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом, а розпорядником таких даних є фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця. Яскравий приклад, який зможе пояснити ці два поняття зазначений у статті 25 Закону України «Про Національну поліцію» поліція в рамках інформаційно-аналітичної діяльності: формує та користується базами (банками) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України. Тобто, володільцем баз даних – буде Міністерство внутрішніх справ України, а розпорядником – Національна поліція. [4]

Згідно Роз’яснення Уповноваженого Верховної Ради України з прав людини від 08.01.2014 року згода суб'єкта персональних даних - добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій чи електронній формі. [3]

Слушним прикладом, надання згоди на обробку персональних даних є проходження реєстрації у соціальну мережу. Оскільки, зареєструватися можна виключно після зазначення ім’я, прізвища, дати народження, місця народження та публікації свого фото.

І тут постає питання, як бути, якщо не хочеться давати згоду на обробку ваших персональних даних? Ніяк. Оскільки текст такої згоди передбачає лише одну опцію – погодитися. [5] Невиконання цієї умови робить неможливими отримання послуги або доступу до певного сайту. У справі №806/3265/17 Велика Палата Верховного Суду звернула увагу, що законодавством не врегульовується питання щодо наслідків відмови особи від обробки її персональних даних, тобто фактично відсутня будь-яка альтернатива такого вибору, що обумовлює низьку якість закону та порушення конституційних прав такої особи. Тобто надання згоди на обробку персональних даних є безальтернативною згодою, що в свою чергу є проблемою.

Основним документом ЄС у сфері захисту персональних даних була Директива 95/46/ЄС Європейського парламенту та Ради Європи від 24 жовтня 1995 року «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (Директива про захист персональних даних).[7]

Але вже у 2018 році вступив у силу Загальний регламент про захист даних (General Data Protection Regulation). Це регламент в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Союзу та Європейської економічної зони.[6]

GDPR замінив Директиву про захист персональних даних і став основою для захисту персональних даних у Європейському Союзі. Згідно регламенту повноваження на захист «приватних» даних покладаються на наглядові органи, які повинні розташовуватися у кожній державі-члені ЄС.

Згідно пункту першого статті 4 Загального регламенту про захист даних персональними даними є будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати. [8]

Пунктом другим статті 4 Регламенту встановлюється поняття опрацювання (обробки) персональних даних і розуміє під собою операцію або низку операцій з персональними даними: збирання, реєстрація, організація, структурування, зберігання, адаптація чи зміна, пошук, ознайомлення, використання, розкриття через передавання, розповсюдження чи надання іншим чином, упорядкування чи комбінування, обмеження, стирання чи знищення.

Відповідно до Регламенту згодою на обробку персональних даних вважається вільне надане, конкретне, поінформоване та однозначне бажання суб’єкта даних підтвердити згоду на опрацювання своїх даних.

Проаналізувавши, правове регулювання захисту персональних даних у законодавстві України та країн Європейського Союзу робимо висновок, що Закон України «Про захист персональних даних» та Загальний регламент про захист

даних, як основні закони захисту персональних даних, є дещо схожими, наприклад у Законі України та Регламенті не вирішена проблема безальтернативності згоди та підстави відмови від надання згоди на обробку «приватних даних». Але у Регламенті встановлені суворіші вимоги до опрацювання персональних даних. Вони полягають в тому, що дані мають збиратися законно, правомірно, прозоро та відповідно до цільового обмеження. Окрім того, їх зберігання обмежується строком, необхідним для опрацювання, яке має відбуватися під захистом від несанкціонованого впливу. За два роки функціонування GDPR наглядовими органами було стягнуто 360 мільйонів євро. Що говорить про те, що, не дивлячись, на проблеми ЄС у справах про захист персональних даних, такий Регламент є дієвим і в подальшому призведе до зменшення кількості порушень. В Україні ситуація є дещо іншою. Оскільки громадяни належним чином не поінформовані про сферу захисту їх персональних даних та система захисту таких даних є досить неефективною. Що і робить нашу країну менш розвиненою у сфері захисту персональних даних.

Література:

1. Конституція України : Закон від 28 червня 1996 р. № 254к/96-ВР. База даних «Законодавство України»/ ВР України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 26.04.2021)

2. Закон України «Про захист персональних даних» : Закон від 01 червня 2010 р. № 2297-VI. База даних «Законодавство України»/ ВР України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 26.04.2021)

3. Роз'яснення Уповноваженого Верховної Ради України з прав людини : Роз'яснення від 08 січня 2014 р. База даних «Законодавство України»/ ВР України. URL: https://zakon.rada.gov.ua/laws/show/n0001715-14#Text (дата звернення 26.04.2021)

4. Шадська Уляна. ТОП-10 питань у сфері захисту персональних даних. 30.10.2019р. URL: https://www.prostir.ua/?library=top-10-pytan-u-sferi-zahystu-personalnyh-danyh (дата звернення 26.04.2021)

5.Фісун Владислав. Проблеми захисту персональних даних: досвід України та інших країн. 29.05.2020р. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html (дата звернення 26.04.2021)

6. Загальний регламент про захист даних. URL: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C

%D0%BD%D0%B8%D0%B9_%D1%80%D0%B5%D0%B3%D0%BB
%D0%B0%D0%BC%D0%B5%D0%BD%D1%82_%D0%BF%D1%80%D0%BE_
%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82_
%D0%B4%D0%B0%D0%BD%D0%B8%D1%85#%D0%92%D0%B8%D0%BA
%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD
%D1%8F_%D0%BF%D1%81%D0%B5%D0%B2%D0%B4%D0%BE%D0%BD
%D1%96%D0%BC%D1%96%D0%B2 (дата звернення 27.04.2021)

7. Посібник з європейського права у сфері захисту персональних даних. Рада Європи . URL: https://rm.coe.int/16805966a8 (дата звернення 27.04.2021)

8. Загальний регламент про захист даних : Регламент від 27 квітня 2016 р. URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf (дата звернення 27.04.2021)

Ніколюк Аліна

Студентка, КПІ ім. Ігоря Сікорського
Науковий керівник: Дубняк М.В.,
к.ю.н., старший викладач
кафедри інформаційного права та
права інтелектуальної власності
КПІ ім. Ігоря Сікорського

ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ

У сучасному світі юристи постійно стикаються із все більшою кількістю нововведень, як у законодавстві, так і у технологіях, з якими, як би іноді нам не хотілося, але доводиться стикатися у своїй професійній діяльності. Адже наразі відбувається стрімка цифровізація усіх практичних аспектів діяльності правника: від судових засідань у режимі відео конференцій, до розробки чат-ботів для надання юридичних послуг. Одним із нововведень, що стали доступними юристам є можливість створення смарт-контрактів. Не можна сказати, що таке нововведення з’явилося зовсім нещодавно, проте природа таких договорів, а, зокрема, і особливості їх укладання як з технічного, так і з правового боків, все ще залишаються проблемними аспектами для багатьох теоретиків та практиків.

Найбільшою перевагою смарт-контрактів є те, що вони значно зменшують витрати для проведення різноманітних транзакцій, мінімізують проблему судового

захисту своїх прав, адже майже прибирають людський фактор та можливі злочинні схеми із порушення умов такого договору. У свою чергу сам смарт-контракт являє собою угоду, прописану за допомогою коду, який автоматично виконує запрограмовані функції у відповідь на певні умови, які виконуються [2]. До елементів смарт-контракту можна віднести: предмет контракту, цифрові підписи, умови контракту та, так звану, децентралізовану платформу. [6].

Отже, навіть на етапі визначення основних елементів смарт-контрактів, ми можемо почати проводити паралелі зі звичайними письмовими договорами, де звично зазначається предмет договору, сторони договору та інші істотні умови. Тож, у такому разі варто звернутися до національного законодавства для визначення того, чи є юридичні відмінності між визначенням поняття та особливостей смарт-контракту та звичного нам договору.

У результаті внесення змін до ст. 205-209 ЦК України у 2015 році, до письмової була прирівняна електронна форма правочину. Дотримання письмової форми правочину стало можливим і у випадку фіксації його змісту у вигляді електронних документів, а також, якщо воля сторін виражена за допомогою телетайпного, електронного або іншого технічного засобу зв'язку. Важливою зміною стало і те, що при його вчиненні стало можливим використання факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, електронно-числового підпису або іншого аналога власноручного підпису, якщо це допускалося законом чи самими сторонами (ст. 207 ЦК України) [1].

Проте, як такого, визначення поняття смарт-контракту в національному законодавстві немає. Що звісно створює безліч проблем із подальшим нормативно-правовим регулюванням правочинів, здійснених таким чином. Тому, у даному випадку Україні варто звернутися до практики інших країн у запроваджені такого інституту, як смарт-контракт.

Тим не менш, і закордоном у багатьох країнах, які активно практикують використання смарт-контрактів, відсутнє легальне визначення цього поняття. І основна проблема полягає у тому, що смарт-контракт можна розглядати з багатьох сторін: як електронний варіант звичайного договору, як код для виконання договірних угод[4], як протокол, що «сприяє, перевіряє, виконує або втілює умови контракту»[5], або ж суто з технічної точки зору, коли поняття смарт-контракту жодним чином не пов’язане з юриспруденцією. Сторони такого договору можуть отримати в обмін на гроші певні товари чи послуги. Як результат, лише ті смарт-контракти, які передбачають обмін, можуть виконати зворотну дію у вигляді оплати. Проте, якщо обмін не відбувається, слід припустити, що термін «смарт-контракт»

використовується в суто технічному сенсі. Звідси і випливає вся складність у формулюванні єдиного законодавчо закріпленого визначення цього терміну.

Однією з основних проблем, яку виділяють науковці із США та Великої Британії, є складність визначення територіальної юрисдикції, у межах якої було укладено такий правочин. Таким чином, важко визначити, законодавство якої країни (якої територіальної одиниці) застосовуватиметься для врегулювання питань, пов'язаних з певним смарт-контрактом, а також до юрисдикції якого суду буде віднесений розгляд спорів, що виникнуть у разі порушення договірних зобов’язань стонами такого смарт-контракту.

Ще одним проблемним аспектом застосування смарт-контрактів ввижається складність реалізації прав сторін такого правочину на правовий захист своїх порушених, оспорюваних або ж невизнаних прав. Науковці, які вказують на те, що смарт-контракти та блокчейни усувають необхідність судового захисту, не враховують того простого факту, що відсутність можливості звернення до встановлених юридичних інститутів не тільки стимулюватиме шахраїв та хакерів, але й перешкоджатиме самому використанню блокчейнів та смарт-контрактів у фінансових операціях. Тут варто зважати і на саму технічну складову смарт-контрактів, яка не може цілком виключати можливості комп’ютерних помилок чи збоїв систем[3].

Тому, враховуючи цю проблему, а також той аспект, що особи, які створюють смарт-контракт, не можуть приймати рішення щодо його комерційних та правових аспектів, то можна припустити, що повинен бути документ, який описує саму суть угоди. Тому, багато смарт-контрактів спершу виникатимуть саме як документи, написані звичайною мовою, і вже потім будуть записані у вигляді коду.

Отже, враховуючи вищезазначений ряд проблемних аспектів як національного, так і міжнародного законодавства, можна прийти до висновку, що попри стрімкий розвиток сучасних технологій та досить тривале існування такого явища, як смарт-контракт, у правовому полі досі існує велика кількість прогалин. Зокрема, основний аспект, на якому варто зосередити увагу – це саме відсутність чіткої визначеності у розумінні самого поняття смарт-контракту, і , як наслідок, неможливість впровадження такого легального терміну у законодавство.

Окрім цього, правове регулювання відносин, що виникають у результаті укладання такого виду угод, наразі не може врахувати усіх особливостей смарт-контракту. Так, все ще залишається відкритим питання визначення територіальних меж вчинення такого правочину, і як наслідок, виникає ряд проблемних питань, щодо застосування положень законодавства певної країни, а також правового захисту, наприклад, звернення до суду.

Література:

1. Цивільний кодекс: Закон України від 16.01.2003 № 435-IV. Відомості Верховної Ради України. 2003. №№ 40-44, ст.356.
2. Andreas Sherborne (2017) Blockchain, Smart Contracts and Lawyers. International Bar Association, c. 3.
3. Jack Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a borderless world (Oxford University Press, 2006) 138.
4. Josh Stark (2016) How Close Are Smart Contracts to Impacting Real-World Law? URL: www.coindesk.com/blockchain-smartscontracts-real-world-law
5. T. Swanson (2014) Great chain of numbers: A guide to smart contracts, smart property and trustless asset management.(“Swanson”) 11, 16.
6. Tar A. Smart Contracts, Explained / A. Tar. URL: https://cointelegraph.com/explained/smart-contracts-explained.

Роженко Андрій

Студент, КПІ ім. Ігоря Сікорського

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УПРАВЛІННЯ ДЕРЖАВОЮ

У наш час інформаційні технології отримали велике значення, вони не могли не торкнутися державного управління та економіки. Завдяки інформаційним технологіям ми отримала не тільки нові способи аналізу, зберігання та бачення справ, а й нові сегменти, яких раніше не було.

Інформаційно-комунікаційні технології (ІКТ) є не тільки одним з найбільш швидко зростаючих галузей - безпосередньо створюючи мільйони робочих місць, але це також є важливим фактором, що сприяє інноваціям та розвитку.

Варто зазначити, що поняття цифрової трансформації сьогодні не має спеціального визначення ні в законодавчих, ні в будь-яких інших правових документах. Відповідно й масив правового забезпечення даного процесу залишається досить невизначеним. Науково-правові дослідження та публікації на тему цифрової трансформації поки що залишаються нечисленними, мало зачіпають як поняття і зміст даного процесу, так і питання його правового забезпечення. Деякі автори, загалом правильно визначивши європейські орієнтири процесу цифрової трансформації в Україні, уважають, що її надалі впроваджую Державне агентство з питань електронного урядування, якого вже не існує. [1]

Інші публікації зачіпають питання цифрової трансформації у вузькому контексті окремих суспільних галузей, зокрема освіти, і не торкаються його суті і змісту як цілісного процесу державно-правового життя України. [2]

Отже, необхідність і актуальність цілісного дослідження та відповідної публікації щодо поняття та правового забезпечення цифрової трансформації в Україні, на наш погляд, не викликає сумнівів. Мета даної публікації полягає в тому, щоб на основі науково-правового дослідження, визначити поняття та правове забезпечення процесу цифрової трансформації в Україні.

Мета данного дослідження полягає в тому, щоб на основі науково-правового дослідження, визначити поняття та правове забезпечення процесу цифрової трансформації в Україні.

Упродовж декількох останніх років в Україні на державному рівні плануються заходи щодо інтенсивного впровадження цифрових технологій в усі сфери суспільного життя. Починаючи від Стратегії сталого розвитку «Україна – 2020»[3], у державі ухвалено низку відповідних концепцій, планів, стратегій, законів та інших нормативно-правових актів. «Цифрові» технології у державному секторі України — це основа його реформування та потенційний приклад для всієї країни, яким чином потрібно використовувати переваги «цифрового» світу. Синергетичний потенціал соціальних, мобільних, «хмарних» технологій, а також технологій аналізу даних та «інтернету речей» у сукупності здатні привести до трансформаційних змін у державному управлінні та загалом, тобто зробити державний сектор України ефективним, реактивним, цінністним.

В умовах становлення «цифрових» ринків та економік, коли громадяни стають фактично користувачами технологій, державні установи повинні робити стратегічні інвестиції в ІКТ. Інакше вони виявляться недостатньо готовими до нових моделей взаємодії та обслуговування, стануть заручниками старих, нестійких в довгостроковій перспективі моделей управління. Повільне, зволікаюче прийняття технологічних інновацій у «цифрову» еру взагалі наражає на риск виконання завдань та досягнення цілей державними установами, їх витрати збільшуються, неефективність зростає, вони все більше стають структурами, котрі не відповідають викликам часу [4].

По-перше, передбачається покращення доступу споживачів та підприємств до товарів і послуг в Інтернеті по всій Європі, що потребує швидкого усунення ключових відмінностей між режимами онлайн і офлайн, щоби зруйнувати бар’єри для транскордонної онлайн-діяльності. По-друге, створення належних умов для розвитку цифрових мереж і послуг, для чого потрібна швидка, безпечна інфраструктура та контентові сервіси, підтримувані правильними регуляторними

умовами для інновацій, інвестицій, чесної конкуренції на рівних умов. По-третє, максимізація потенціалу зростання європейської цифрової економіки, для чого необхідне використання інфраструктури та технологій ІКТ, як-от хмарні обчислення та великі дані, досліджень та інновацій для підвищення конкурентоспроможності промисловості, а також поліпшення державних послуг, інклюзивності та навичок. Зауважимо, що значна частина положень Стратегії спрямовані на подолання міждержавних бар'єрів усередині Європейського Союзу (далі – ЄС), таких, зокрема, як геоблокування, відмінності в регулюванні радічастотного ресурсу, поштових відправлень тощо. У контексті європейської стратегії варто згадати про значення Угоди про асоціацію з ЄС Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27 червня 2014 р.[5]

Розглянемо директивні документи сфери цифрової трансфомації, оскільки саме вони містять базові філософські, політичні, правові й організаційні положення, що стають основою для нормативних настанов і подальшої практичної реалізації. Одне із провідних місць тут належить Стратегії єдиного цифрового ринку для Європи (A Digital Single Market Strategy for Europe) [6].

Як одному з перших хронологічно та як визначальному спеціальному документу з погляду європейської цифрової стратегії України. Цей документ підготовлений Європейською комісією у 2015 р. і визначає три базові опори єдиного цифрового ринку Європи. По-перше, передбачається покращення доступу споживачів та підприємств до товарів і послуг в Інтернеті по всій Європі, що потребує швидкого усунення ключових відмінностей між режимами онлайн і офлайн, щоби зруйнувати бар'єри для транскордонної онлайн-діяльності. По-друге, створення належних умов для розвитку цифрових мереж і послуг, для чого потрібна швидка, безпечна інфраструктура та контентові сервіси, підтримувані правильними регуляторними умовами для інновацій, інвестицій, чесної конкуренції на рівних умов. По-третє, максимізація потенціалу зростання європейської цифрової економіки, для чого необхідне використання інфраструктури та технологій ІКТ, як-от хмарні обчислення та великі дані, досліджень та інновацій для підвищення конкурентоспроможності промисловості, а також поліпшення державних послуг, інклюзивності та навичок. Зауважимо, що значна частина положень Стратегії спрямовані на подолання міждержавних бар'єрів усередині Європейського Союзу (далі – ЄС), таких, зокрема, як геоблокування, відмінності в регулюванні радічастотного ресурсу, поштових відправлень тощо. У контексті європейської стратегії варто згадати про значення Угоди про асоціацію з ЄС цифрової трансформації в Україні.Угода про асоціацію між Україною, з однієї сторони, та

Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27 червня 2014 р. [5] В мене є власна думка щодо регулювання та пропозиції щодо забезпечення цифрової трансформації управління державою. Для впровадження ініціатив щодо трансформації державних організацій через «цифровізацію» нижче наведено 10 головних стратегічних технологій, точніше перелік стратегічних технологій, багато з яких вже відповідають українським реаліям та можуть використовуватися на шляху трансформації та реформування.

Отже, 10 головних стратегічних технологій для державного сектору України:

1) «Цифрове» робоче місце
2) Багатоканальне інформування та залучення громадян
3) Відкриті дані
4) Електронна ідентифікація громадян
5) Повсюдна аналітика
6) «Розумні» машини та засоби
7) «Інтернет речей»
8) «Цифрові» державні платформи
9) Програмні архітектури (програмно-конфігуровані архітектури)
10) Блокчейн (Blockchain)

У вересні 2017 р. Кабінет Міністрів України (далі –КМУ) схвалив Концепцію розвитку електронного урядування в Україні. [7] Яка визначила Електронне урядування як форму організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади й органів місцевого самоврядування з використанням інформаційно телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян. В основу реалізації системи електронного урядування було покладено такі принципи: цифровий за замовчуванням; одноразове введення інформації; сумісність за замовчуванням; доступність і залучення громадян; відкритість та прозорість; довіра та безпека. Досягнення мети Концепції забезпечувалось виконанням комплексних заходів за такими напрямами, як: модернізація публічних послуг та розвиток взаємодії влади, громадяні бізнесу за допомогою інформаційно-комунікаційних технологій; модернізація державного управління за допо- могою інформаційно-комунікаційних технологій; управління розвитком електронного урядування. Варто відзначити, що дана Концепція відрізняється від аналогічних попередніх документів вищим рівнем деталізації та комплексним характером. Для її впровадження був ухвалений. План заходів із реалізації Концепції розвитку електронного урядування в Україні. [8]

Отже, додержуючись та ретельно виконуючи теоретичні засади відповідних Законів, Постанов, Програм, Концепцій тощо, цілком можливо зробити значний крок до якісно нової дійсності, а це означає, що окремі особи та великі об'єднання, громади та й, зрештою, цілі народи мають реальну перспективу повною мірою реалізувати свій потенціал, жити комфортно, відчуваючи, що влада й справді дбає про свій народ.

Саме таке інформаційне суспільство, орієнтоване на інтереси людей, відкрите для всіх і спрямоване на загальний розвиток держави, є кінцевою метою стратегії України у сфері інформаційно-комунікаційних технологій.

Цифрові трансформації в державному секторі України – це основа його реформування та приклад для країни, яким чином потрібно використовувати переваги «цифрового» світу, котрі будуть стимулювати розвиток відкритого інформаційного суспільства як одного з істотних чинників розвитку демократії в Україні, підвищення продуктивності, економічного зростання, створення робочих місць, а також підвищення якості життя громадян України.

Література:

1. Духовна О. Україна «в цифрі» : напрямки реформування. *Юридична газета online.* URL: http://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ukrayina-v-cifri-napryamki-reformuvannya.html.

2. Бабаєв В., Стадник Г., Момот Т. Цифрова трансформація у сфері вищої освіти в умовах глобалізації. Комунальне господарство міст. 2019. Т. 2. № 148. URL: https://khg.kname.edu.ua/index.php/khg/issue/view/115.

3. Про Стратегію сталого розвитку «Україна – 2020» : Указ Президента України від 12 січня 2015 р. № 5. URL: https://zakon.rada.gov.ua/ laws/show/5/2015.

4. Hitech office (2016), "Digital Agenda of Ukraine 2020 (Digital Agenda 2020): Conceptual Framework (Version 1.0). Priority Areas, Initiatives, Digitization Projects of Ukraine by 2020: Project", available at: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf (Accessed 25 Oct 2019)

5. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27 червня 2014 р.URL: http://zakon5.rada.gov.ua/laws/show/984_011.

6. A Digital Single Market Strategy for Europe: Communication from the Comission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. URL: [6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex-%3A52015DC0192

7. Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження КМУ від 20 вересня 2017 р. № 649-р. URL:https://zakon.rada.gov.ua/laws/show/649-2017-р.,
8. Про затвердження плану заходів з реалізації Концепції розвитку електронного урядування в Україні : розпорядження КМУ від 22 серпня 2018 р. № 617-р. URL: https://zakon.rada.gov.ua/laws/main/617-2018-р., де визначались завдання для відповідних міністерств.

Розгон Ольга

к.ю.н., доцент, провідний науковий співробітник, НДІ правового забезпечення інноваційного розвитку НАПрН України

НЕОБХІДНІСТЬ УРЕГУЛЮВАННЯ КАТЕГОРІЙ АВТОНОМНІ РОБОТИ І ШТУЧНИЙ ІНТЕЛЕКТ У РОЗРІЗІ ДИСКУСІЇ КОНЦЕПЦІЇ ОНОВЛЕННЯ ЦК УКРАЇНИ

Наразі відбуваються дискусії з приводу внесення змін та доповнень до чинного ЦК України, які спрямовані на удосконалення цивільно-правового регулювання відносин, у тому числі усунення існуючих прогалин і невідповідностей. Ці зміни стосуються зокрема питань *штучного інтелекту.*

Посідає важливе місце у правовому регулюванні цієї правової категорії *Концепція розвитку штучного інтелекту в Україні*, яка була схвалена Кабінетом Міністрів України від 02.12.2020 р. № 1556-р. Концепція визначає ключові напрями державної політики у сфері штучного інтелекту: освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека, оборона, публічне управління, правове регулювання та етика правосуддя.

У Концепції оновлення ЦК України до Книги першої. Загальні положення (Розділ і основні положення. Глава 1. Цивільне законодавство України) пропонується внести зміни з позиції усвідомленої відповідальної взаємодії людини з *автономними роботами і штучним інтелектом*.

Підтримуємо такі зміни, оскільки застосування сучасних передових *технологій штучного інтелекту, автономних роботів* не повинне суперечити правам людини, громадянським свободам, принципам верховенства права. Отже, використання і розробки штучного інтелекту та автономних роботів, а також пов’язаних із цим питань має бути із дотриманням фундаментальних прав людини в

Україні, які зазначені у Конвенції про захист прав людини та основоположних свобод (ЄКПЛ).

Друга позиція Концепції оновлення ЦК України, яка заслуговує на увагу, — неприпустимість втручання в особисте життя фізичної особи, що обумовлене розвитком *новітніх технологій, як-от штучний інтелект*, які необхідно розвинути в окремій Книзі ЦК України щодо неприпустимості свавільного втручання у сферу інформації про особу, персональних даних та ін.

Підтримуємо такі зміни на підставі необхідності *захисту особистих немайнових прав людини.* Необхідно зазначити, що у ст. 200 ЦК України під інформацією маються на увазі будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Суб'єкт відносин у сфері інформації може вимагати усунення порушень його права і відшкодування майнової та моральної шкоди, завданої такими правопорушеннями. Порядок використання інформації та захисту права на неї *встановлюється законом*. Тобто Законом України «Про інформацію», яка містить ст. 11, що стосується інформації про фізичну особу. У ній зазначено, що *інформація про фізичну особу (персональні дані)* — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Отже, необхідно, визначаючи «неприпустимість свавільного втручання у сферу інформації про особу, персональних даних та ін.» як засаду чи принцип, ураховувати і те, що у цій трактовці принцип зустрічається у чинному ЦК України (наразі, наприклад, у ст. 200), а також внести зміни до тих нормативно-правових актів, які пов'язані з питанням неприпустимості свавільного втручання у сферу інформації про особу, персональних даних та ін. через застосування *новітніх технологій, як-от штучний інтелект*.

До найактуальніших проблем належить порушення прав людини, зокрема, викликане свавільним втручанням у *сферу інформації про особу, персональних даних* та ін. Так, користування додатками і соціальними мережами із *застосуванням новітніх цифрових технологій, як-от штучний інтелект*, дозволяє збирати персональні дані (з обізнаністю людини або без неї). Використання *штучного інтелекту* може призвести до *дискримінації* у судових рішеннях, а ст. 14 ЄКПЛ вказує на заборону дискримінації. Цей висновок базується на тому, що технології штучного інтелекту можуть містити расові та гендерні стереотипи.

Отже, використання штучного інтелекту ставить під загрозу свободу висловлювання думок, отримання інформації, думки і переконань, що пов'язано з масштабним збиранням персональних даних, їх неналежним впливом на думку людини. З метою недопущення порушення прав людини необхідно, працюючи над

проєктом внесення змін та доповнень до чинного ЦК України, врахувати як «позитивні сторони» штучного інтелекту, так і загрози, які можуть виникнути при його використанні.

Третя позиція, яка стосується урегулювання категорії «автономні роботи і штучний інтелект» у ЦК України, — розширення переліку об'єктів цивільних прав. Положення ЦК України щодо об'єктів цивільних прав пропонується розширити, заважаючи на розвиток цивільного обороту і появу в ньому невідомих на момент створення ЦК України об'єктів. Передусім ідеться про такі об'єкти: інформаційні продукти, інформаційні ресурси, інформаційні системи тощо; об'єкти прав, що створюються і знаходяться у мережі «Інтернет»; криптовалюта; персональні дані, інформація про особу; *автономні роботи, штучний інтелект*, цифровий контент тощо.

Підтримуємо розширення переліку об'єктів цивільних прав і включення до нього, зокрема, *автономних роботів і штучного інтелекту*.

У програмі Industry 4.0. передбачається впровадження у виробництво нових цифрових технологій, таких як робототехніка, штучний інтелект (AI) тощо.

Але зауважимо, що *робот* — це предмет матеріального світу. Однак існує думка, що робот — це не завжди фізичний механізм, оскільки одним із видів роботів є софтверні (роботи-програми, які вміють взаємодіяти з об'єктами реального світу і давати відчутний результат). *Інтелектуальний робот* — це не форма штучного інтелекту, а автоматичний пристрій, механізм, *наділений «штучним інтелектом»*, тобто «робот розумний», а формою штучного інтелекту є, наприклад, нейромережі.

Серед вчених порушується питання про розгляд *штучного інтелекту як нового об'єкта інтелектуальної власності*. У матеріалах Всесвітньої організації інтелектуальної власності (ВОІВ) визначені певні сфери діяльності де використовується штучний інтелект. Зокрема, автоматична класифікація патентів і товарів/послуг, патентний пошук, експертиза і перевірка дотримання формальних вимог для товарних знаків і патентів, функція автоматичного клієнта, машинний переклад, лінгвістичні інструменти і термінологія, аналіз даних для економічних досліджень.

Штучний інтелект як одна з технологій і невід'ємна частина в Industry 4.0. тлумачиться як термін, використовуваний для опису машин, що виконують когнітивні функції, подібні людським, такі як навчання, розуміння, міркування або взаємодія [1].

Згідно з висновками International Telecommunication Union (ITU) у 2018 році *штучний інтелект* включає 5 видів технологій: комп'ютерний зір, відтворення

мови, віртуальні помічники, автоматизована (робототехнічна) робота і сучасне машинне навчання.

На даному етапі розвитку штучного інтелекту основні дискусії серед вчених відбуваються з питань виняткового права, авторства на згенерований контент, розгляду його як об’єкта інтелектуальної власності [2].

Отже, використання технологій штучного інтелекту (як цифрова технологія, об’єкт інтелектуальної власності) і розвиток робототехніки (як предмет матеріального світу) сприяє впливу на суспільні відносини і викликає загрозу порушень прав людини. Відповідно, слід створити правила регулювання застосування штучного інтелекту як цифрової технології, а також робототехніки.

Література:

1. Industry 4.0. A Policy Brief from the Policy Learning Platform on Research and innovation. September 2019.

2. Амбариян Е. Г. Робототехника, искусственный интеллект и интеллектуальные права / Е. Г. Амбариян, Т. Ж. Чубарова. *Юный ученый*. 2018. № 3(17). С. 66–69. URL: https://moluch.ru/young/archive/17/1253.

Строк Анастасія

Студентка, КПІ ім. Ігоря Сікорського

ШТУЧНИЙ ІНТЕЛЕКТ В ЮРИСПРУДЕНЦІЇ: ПЕРСПЕКТИВИ ТА РИЗИКИ

Соціальний світ в XXI столітті зазнає глобальної трансформації. Формування інформаційного суспільства, розвиток сучасних технологій, створення штучного інтелекту - поставили нові проблеми перед людством, в тому числі і перед юридичним світом, як дуже значущою частиною його буття. Для гуманітарного знання, юридичної освіти, професії юриста і в цілому юриспруденції, розвиток сучасних технологій і створення штучного інтелекту - один з основних викликів сучасного суспільства. Чи може штучний інтелект «перемогти» природний і змінити або в перспективі замінити багато професій, в тому числі, як переконані деякі автори, і юридичні? Чи всі види правової діяльності можуть бути замінені роботами, які перспективи стійкості юридичної професії на ринку праці? Не володіючи спеціальними знаннями в області штучного інтелекту, спробую з позиції гуманітарного знання розібратися в цій складній проблемі і представити своє бачення модернізації правової сфери в XXI столітті [4].

Перш за все, слід отримати відповіді на ключові, на мій погляд, питання: як слід ставитися до нових технологій та впровадження штучного інтелекту в юриспруденцію? Чи призведе цей процес до конкуренції на ринку праці і заміни деяких категорій юридичної професії юристами-роботами, як оцінити можливі ризики застосування штучного інтелекту в юридичній сфері? Проблема активно обговорюється в юридичному співтоваристві: палітра думок розходиться від консервативного ставлення до технологічних новацій до досить зваженого сприйняття і передбачення позитивних ефектів в можливості використання штучного інтелекту в юридичній практиці [4].

Штучний інтелект - термін, що використовується для комп’ютерного алгоритму, який може аналізувати, розробляти стратегії та робити висновки для подальшого виконання завдань, які зазвичай виконуються людьми. Хоча штучний інтелект є відносно новим поняттям, люди мріяли використовувати здатність комп’ютерів допомагати у виконанні юридичних завдань протягом сотень років. Наприкінці 1600-х років німецький філософ Готфрід Вільгельм Лейбніц висунув теорію, що машини колись використовуватимуть двійкову логічну систему для обчислення чисел, і він передбачав партнерство між штучним інтелектом та юристами. Попри те, що він ніколи не бачив нічого схожого на комп'ютер, він точно описав переваги, які зараз надає штучний інтелект юридичній професії: «Недостойно, для чудових людей втрачати години, як раби, під час розрахунків, які можливо було б, безпечно передати комусь іншому, як би машини були спроможні на таке» [2].

Мобільні додатки для юристів, аналітичні онлайн-платформи, онлайн-конструктори договорів, розумні офіси юридичних фірм - все це вже активно працює в юридичному полі. Програмне забезпечення на основі штучного інтелекту дозволяє юридичним фірмам автоматизувати завдання більш низького рівня, звільняючи час для юристів, за для зосередження на комплексному аналізі справи та взаємодії з клієнтами. Штучний інтелект значно розширює можливості адвоката досліджувати, консультувати і обслуговувати своїх клієнтів. Деякі великі фірми вже використовують інструменти на основі штучного інтелекту для поліпшення своєї практики. Згідно з дослідженням, проведеним Міжнародною асоціацією юридичних технологій за 2019 рік, 100 з 700 і більше юридичних фірм вже використовують інструменти штучного інтелекту або реалізують проекти в даній області [3].

В даний час, в умовах інноваційної економіки та інформаційного суспільства, коли замовлення і аналіз документів виконуються автоматично, завдяки роботизації і цифрових технологій (наприклад: складання позовних заяв, договорів, претензій тощо), вартість юридичних послуг знижується, що є вигідним для клієнтів і як

наслідок, викликає конкуренцію серед юристів за першість, що покращує якість наданих послуг. Також, фірми, особливо великі підприємства, які не пристосовуються до мінливих технологій, скоро будуть щосили намагатися конкурувати.

Однак, не лише особисто юристи та фірми, починають використовувати новітні розробки, все частіше штучний інтелект використовується і в державних установах. Наприклад, Міністерство юстиції України починає використовувати програмне забезпечення "Касандра" з елементами штучного інтелекту, що надає можливість аналізувати ймовірність повторного порушення закону конкретним злочинцем. Покарання за злочин встановлює суд, але для того, щоб йому допомогти в цьому, існує документ під назвою "Досудова доповідь", який готують співробітники пробації. Це частина Міністерства юстиції. У цьому документі описується особистість обвинувачуваного, а також оцінка ймовірності вчинення ним нових злочинів. Відповідно "Касандра" цей процес автоматизує [5]. Співробітник, відповівши на запитання, котрі встановлені даною програмою, отримує оцінку ймовірності вчинення нового злочину від 0 до 97. Ця оцінка проводиться за допомогою алгоритму, який надає бали за конкретне питання, а потім підсумовує їх.

Найбільш очевидним недоліком використання вищезазначеної програми є те, що рішення ґрунтуються лише на відомих даних. Якщо злочинець не був раніше судимим, його "профіль" буде чистим, тому програма вважатиме ймовірність можливого повторення правопорушення, відповідно меншою. Також, через нелінійність та неоднорідність даних неможливо побудувати ефективні алгоритми оцінки. Уявімо, є злочинець, якого шукали кілька років, котрий вчинив декілька злочинів. Але за ці кілька років, його життя сильно змінилося - він став релігійною людиною, створив сім'ю, зайнявся благодійністю. Звичайно, це не гарантія, але ймовірність втечі чи повторного вчинення злочину може бути значно зменшена. Інший приклад - колишній поважний і добрий вчитель, багатодітний батько та сумлінний платник податків, який пішов слизьким шляхом і розпочав виробництво метамфетаміну з усіма кримінальними наслідками такої діяльності. Що скаже машина? Додаткових умов може бути багато. Ефективність програми полягає виключно на застосуванні загальних моделей алгоритмізації, виключаючи будь-які інші елементи, які не відповідають їм [1].

Однак, окрім недоліків використання штучного інтелекту, також має ряд переваг. Подолання людських помилок - одна з них. Значна кількість когнітивних упереджень притаманна людям. Нобелівський лауреат Даніель Канеман, дослідник поведінкової економіки, у своїй книзі "Думай повільно…вирішуй швидко" описав близько 25 найпоширеніших психологічних помилок, які люди роблять при оцінці

фактів і прийнятті рішень. Штучний інтелект позбавлений цих недоліків людської психіки, принаймні теоретично, здатний надати набагато більш об'єктивний результат аналізу складного комплексу фактів і прийняти більш раціональне рішення. Якщо взяти до уваги, що штучний інтелект не має емоцій, не може відчувати симпатію чи антипатію до людини, то ми отримаємо очевидно більш справедливого та незалежного суддю [1].

Отже, оцінивши усе вище вказане, результуюче питання: як реагувати на «інтервенцію» штучного інтелекту в область юриспруденції?

Використання штучного інтелекту піднімає широкий спектр юридичних, психологічних, філософських і етичних питань. Будь-які розробки в галузі інтелектуальних технологій повинні працювати виключно на благо людства. При створенні нових програм з використанням штучного інтелекту необхідно одночасно розробити певний перелік правил поведінки для їх використання, який необхідний для запобігання та мінімізації ризиків зловживання цією технологією, і Також, особливу увагу слід приділити законодавству у сфері захисту персональних даних, захисту інформації, інтелектуальної власності і конкуренції.

Крім того, у стратегії юридичної освітньої системи, акцент слід поставити, по-перше на вивчення сучасних інформаційно-комунікаційних технологій. По-друге, слід приділити увагу, на підготовку елітарної групи спеціалістів, що володіють знаннями та компетенціями юристів та ІТ-спеціалістів, здатних спільними зусиллями розробити цифрові програми, алгоритми, що найбільш ефективно впливають на результати юридичної діяльності. Розробка техніко-гуманітарної підготовки даних спеціалістів підсилює їх вклад у технологічну сферу юриспруденції та буде мінімізувати риски, пов'язані з введенням в правову систему штучного інтелекту [4].

Література:

1. Legal Regulation of the Use of Artificial Intelligence: Problems and Development Prospects. *European Journal of Sustainable Development* (2021) P. 281-289. Doi:10.14207/ejsd.2021.v10n1p281

2. M. Ridgway. Barker Artificial Intelligence will advance the practice of law, but it introduces the potential for discrimination and liability. URL: https://www.withersworldwide.com/en-gb/insight/artificial-intelligence-will-advance-the-practice-of-law-but-it-introduces-the-potential-for-discrimination-and-liability

3. Rachel Vanni. How Artificial Intelligence Is Transforming the Legal Profession. URL: https://kirasystems.com/learn/how-artificial-intelligence-is-transforming-the-legal-profession/

4. А. А. Соколова Искусственный интеллект в юриспруденции: риски внедрения. *Ежегодник «Юридическая техника»*. 2019. № 13 С. 350-356.

5. УКРІНФОРМ. URL: https://www.ukrinform.ua/rubric-technology/3098629-stucnij-intelekt-dopomoze-uniknuti-povtornih-zlociniv-minust-zapuskae-kasandru.html

Стужук Ольга

Студентка, КПІ ім. Ігоря Сікорського

ВПРОВАДЖЕННЯ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У НАЦІОНАЛЬНОМУ ЗАКОНОДАВСТВІ

На сьогодні інформаційні технології не стоять на місці. Навпаки, вони активно рухаються вперед. Вони стають все більш повсякденними і використовуваними в нашому житті. Технології штучного інтелекту розвиваються, в тому числі через розвиток технологій стійких нейронних мереж та інфраструктур хмарних обчислень, технологій нечітких систем, ройового інтелекту, еволюційних обчислень та інше. Ця стаття присвячується розслідуванню того, як застосовується штучний інтелект в національному та світовому законодавств

Через початок активного залучення нових технологій та штучного інтелекту в сферу правосуддя виникає багато невирішених питань. У 2018 році Європейська комісія з ефективності правосуддя Ради Європи прийняла новий міжнародний акт — Етичну хартію по використанню штучного інтелекту у судовій системі та її середовищі. На меті цієї хартії підвищити ефективність, якість та безпеку, захистити основні права та свободи людства. [2]

Близько півроку тому міністерство юстиції України створило штучний інтелект, який аналізуватиме злочинців. “Касандра” повинна визначати процент можливого вчинення нового злочину в майбутньому, автоматизувати підготовку досудової доповіді. В цій доповіді б вказувались особливості обвинуваченого та ймовірність вчинення нових злочинів. Це б могло дуже допомогти суддям вирішити багато питань. “Касандра” пропонує обвинуваченому певний тест в якому потрібно відповідати на запитання і в залежності від відповіді потім виставляються бали і вираховується можливість скоєння нового злочину. [1]

2 грудня 2020 року Кабінет Міністрів України схвалив Концепцію розвитку штучного інтелекту в Україні та доручив Міністерству цифрової трансформації в тримісячний термін розробити план реалізації цієї концепції. Згідно з текстом

доповідної записки до розпорядження, концепція спрямована на підвищення конкурентоспроможності України завдяки використанню технологій штучного інтелекту в багатьох важливих сферах важливих для країни. [3] [4]

Відмінність та гарна риса сучасної обробки даних полягає в тому, що вона не намагається відтворити розумові процеси людини, а розробляє статистику на основі даних та без можливих помилок, які б могла ненароком допустити людина. Згадаємо найбільш використовувану програму в системі кримінального правосуддя США. Це програмне забезпечення COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) — продукт комерційної компанії "Northpointe" (з 2017 року компанія має назву "Equivant"). Вона оцінює ризик повторного злочину і допомагає цим судді укласти вирок. Програми не можуть оцінити всю ситуацію з точки зору людини, вони лише аналізують дану їм інформацію. На замовлення Національної довідкової служби з кримінального правосуддя США було проведено дослідження. Воно показало нам, що штучний інтелект може допомогти нам не тільки в затриманні злочинців, а і в запобіганні злочинів. Хоч це й робота поліцейських, в теорії програма може впоратися не гірше. Проте на практиці можуть виникнути нові проблеми, а в випадку успіху це забере роботу в багатьох поліцейських. [2]

Користь штучного інтелекту можна розглядати з декількох сторін. Це відкриває нові можливості, пришвидшує весь процес, але й забирає роботу в людей, знищує професії. Україна має найбільшу кількість компаній-розробників штучного інтелекту в Східній Європі. Тому є дуже важливим розробити зрозумілу для держави та приватного сектору стратегію розвитку штучного інтелекту в нашій країні. Це незворотньо виводить нас на новий рівень цивілізації і нікому не відомо, яка кількість людей зможе пристосуватися та звикнути до цього. Чим взагалі це може закінчитися в подальшому.

Література:

1. Фейсбук. Denis Malyuska URL: https://www.facebook.com/100011121947008/videos/1230395760674477/ (дата звернення 24.04.2021)

2. Центр демократії та верховенства права. ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВОСУДДІ. URL: https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/ (дата звернення 23.04.2021)

3. Укрінформ. В Україні схвалили план розвитку штучного інтелекту до 2030 року. URL: https://www.ukrinform.ua/rubric-technology/3147236-v-ukraini-shvalili-plan-rozvitku-stucnogo-intelektu-do-2030-roku.html (дата звернення 23.04.2021)

4. Урядовий портал. Про схвалення Концепції розвитку штучного інтелекту в Україні. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220 (дата звернення 24.04.2021)

Ткаченко Анна

Студентка, КПІ ім. Ігоря Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ

Стрімкий розвиток новітніх розробок, зокрема штучного інтелекту, сприяє їхньому запровадженню у суспільне життя. З огляду на це, перед юристами постає важливе питання забезпечення правового регулювання технологій штучного інтелекту для подальшого розв’язання типових задач, що можуть виникнути в даній сфері. Значних звершень досягли в цьому напрямі такі країни як: Японія, Німеччина, Південна Корея, США. Розуміючи перспективність впровадження цього і важливість Україна також розпочала план інтеграції.

Перш за все, для повноцінного та дієвого розуміння змісту даної галузі, варто схарактеризувати поняття штучного інтелекту. Провідними науковцями та дослідниками-практиками у цій галузі було запропоновано безліч пропозицій з можливими варіантами відповідного терміну. Зокрема, Баранов О.А. викладає поняття так: «Штучний інтелект – це певна сукупність методів, способів, технологій і засобів, в тому числі, апаратних, та комп'ютерних програм, які реалізують одну, кілька або всі когнітивні функції, які є еквівалентними когнітивним функціям людини» [1, с. 10-11]. Водночас, Спірін О.М. тлумачить штучний інтелект як: «науковий напрямок, у рамках якого ставляться і розв’язуються задачі апаратного або програмного моделювання тих видів людської діяльності, які традиційно вважаються інтелектуальними» [2, с 124].

Незважаючи на відсутність одностайності рішення щодо сталої та повної в змістовному значенні дефініції, в іноземних країнах вже були проведені певні спроби інтерпретації. Європейський Парламент 16 лютого 2017 р. ухвалив Резолюцію 2015/2103(INL) щодо цивільно-правового регулювання робототехніки з рекомендаціями для Європейської Комісії. Серед основних положень змісту також бралося до уваги формування однозначних термінів, які повинні були б містити такі ознаки робота, який має інтелект: можливість бути автономними й обмінюватися даними, а також проводити їхній аналіз; здатність до самонавчання на основі набутого досвіду і взаємодії з навколишнім світом; наявність мінімальної матеріальної допомоги; вміння адаптації до зовнішнього середовища; відсутність життя в біологічному розумінні [3].

Україна, перебуваючи у складі членів Спеціального комітету зі штучного інтелекту при Раді Європи, приєдналася у жовтні 2019 року до Рекомендацій

Організації економічного співробітництва і розвитку з питань штучного інтелекту (Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449). І вже 2 грудня 2020 року Кабінетом Міністрів України було схвалено план Концепції розвитку штучного інтелекту, одне із завдань якого полягає у формуванні українського законодавства у сфері впровадження, використання та регулювання технологій штучного інтелекту відповідно до стандартів міжнародних нормативно-правових актів та актів європейського правового середовища.

В Концепції застосовується використання терміну штучний інтелект як: «організованої сукупності інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань»[4]. Таким чином, підкреслюючи значення європейської інтеграції та політико-правових реформ для нашої держави.

Відповідно до інших її положень, Україна також повинна здійснити імплементацію норм, закріплених у “Рекомендаціях щодо штучного інтелекту”, що прийняті у червні 2019 року Організацією економічного співробітництва та розвитку (OECD/LEGAL/0449), а також розробити Етичний кодекс штучного інтелекту[4].

Відтак, Україна лише розпочинає втілення правового регулювання технологій штучного інтелекту і має рекомендаційний та декларативний характер. Тобто, розробка відповідних технологій та правового середовища, у якому буде діяти штучний інтелект, як суб’єкт або об’єкт правовідносин, знаходиться на ранній стадії у зв’язку з повільними темпами розвитку інших галузей знань та їх втілення в практику через недоліки функціонування державного механізму.

Слід зазначити, що опрацювання концепту запровадження правового регулювання технологій штучного інтелекту вже місять роботи таких дослідників як О. А. Баранов, К. В. Єфремова, О. М. Спірін, Є. О. Харитонов, О. І. Харитонова та інших. Серед основних пропозицій дослідників та стандартів міжнародного законодавства у робототехніці присутні ідеї:

– визначення уповноваженого державного суб’єкта права, компетенція якого полягатиме у регулюванні штучного інтелекту, за допомогою встановлення стандартизованих правових норм;

– визначення правового статусу штучного інтелекту у правовідносинах інтелектуальної власності та його становища у правовідносинах загалом;

– розроблення механізмів державної реєстрації та механізмів державного контролю, що змогли б здійснювати охорону, попередження та надання прав на основі відповідного статусу з можливістю проведення ідентифікації штучного інтелекту та міжнародної співпраці;

– формування спеціального виду правосуб'єктності на основі обумовленості нових факторів, що вводять нові характеристики для взаємодії між учасниками в IT-сфері;

– розроблення термінологічного словника, який би містив визначення всіх технічних і техніко-юридичних аспектів галузі, що застосовуватимуться в законодавчих положеннях та дефініціях; [5, 162 с.]

Література:

1. Баранов О.А., Інтернет речей і право: погляд у майбутнє. *Інтернет речей: проблеми правового регулювання та впровадження* : матеріали третьої наук.-практ. конф. (м. Київ, 21 листопада 2019 р.). Київ, 2019. 10-11 с.

2. Спірін О.М. Початки штучного інтелекту : Навчальний посібник для студ. фіз.-мат. спец-тей. Вищих пед. навч. закладів. Житомир: Вид-во ЖДУ, 2004. 172 с.

3. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). European Parliament Official web-site. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (дата звернення: 21.04.2021).

4. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 21. 04. 2021).

5. Костенко О.В., Костенко В.В. Правова відповідальність та ідентифікація суб'єктів і об'єктів зі штучним інтелектом (іот) : *Юридичний науковий електронний журнал*. 2020. № 1. 158-162 с.

Ткачук Тарас

д.ю.н., доцент, Національна академія
Служби Безпеки України

Пономаренко Ірина

Аспірант, Національна академія
Служби Безпеки України

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ ПРИВАТНОСТІ У МЕДИЧНІЙ СФЕРІ УКРАЇНИ ТА США

Забезпечення інформаційної приватності у медичній сфері України набуло актуальності після прийняття Закону України «Про захист персональних даних». Зокрема, ст. 7 заборонено обробку персональних даних, яка проводиться в цілях охорони здоров'я, встановлення медичного діагнозу, з метою забезпечення піклування чи лікування або надання медичних послуг за умови, що такі дані обробляються медичним працівником або іншою особою медичного закладу охорони здоров'я, на якого покладено обов'язки щодо захисту персональних даних та на якого поширюється законодавство про лікарську таємницю [1]. На думку Г.О. Блінової, «… сформулювавши таку норму, законодавець встановив подвійний механізм захисту медичної інформації про стан здоров'я пацієнта: в режимі лікарської таємниці та в режимі персональних даних» [2, с. 136]. Разом з цим варто звернути увагу на те, що у деяких нормативно-правових актах поряд із поняттям «лікарська таємниця» використовується поняття «медична інформація». Таким чином виникає ситуація, за якої захист однієї і тієї ж інформації проводиться у межах різних правових режимів – лікарської, медичної таємниць та персональних даних.

Варто зазначити, що у вітчизняному законодавстві відсутнє нормативне визначення поняття «медична таємниця», а в деяких випадках вживається поняття «лікарська таємниця». З цього приводу у науці права тривають дискусії. Одні вчені (В. Головченко, Л. Грузова, І Купова, І. Петрухіна) вважають, що лікарська таємниця – один із видів медичної таємниці. Інші (А. Марущак, М. Хавронюк) притримуються позиції, що це абсолютно різні поняття. Який же із цих двох термінів більш прийнятний для використання? М.І. Мельник та М.І. Хавронюк у Науково-практичному коментарі до Кримінального кодексу України наголошують: «лікарська таємниця (інформація про пацієнта), відрізняється від медичної таємниці (інформації для пацієнта), яка передбачає відомості про стан здоров'я людини, історію її хвороби, мету запропонованих досліджень і лікувальних заходів, прогноз

можливого розвитку захворювання, які лікар зобов’язаний надати на вимогу пацієнта, членів його сім’ї або законних представників, за винятком випадків, коли така повна інформація може завдати шкоди здоров’ю пацієнта» [3, с. 332]. Отже, основним критерієм поділу інформації на ці два види науковці визнають мету її збереження та використання. На думку С.Г. Стеценка поняття «лікарська» не зовсім точно відображає обов'язок збереження у таємниці інформації про хворого. Більш точним може вважатися використання терміна «медична таємниця», оскільки мова йде про всю сферу медицини, про необхідність не тільки лікарям зберігати в таємниці отримані відомості. Тим більше, зважаючи на стрімкий розвиток інформаційних технологій, реформи у сфері медицини, комплексний характер сучасної медичної допомоги призводить до того, що така конфіденційна інформація часто стає доступною не лише лікарям, а й представникам інших професій [4]. Даної наукової позиції притримуються і І.Я. Сенюта та Г.О. Блінова. З урахуванням зазначеного, а також зважаючи на те, що поняття «медична таємниця» набагато ширше, ніж поняття «лікарська таємниця», доцільно звести термінологічний апарат у даній сфері до терміна «медична таємниця».

Відповідно до Конституції України: «Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» (ст. 32) [5]. Цивільним кодексом України (ч. 1 ст. 286) та Основами законодавства України про охорону здоров’я (ч. 1 39-1) передбачено: «… фізична особа має право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при її медичному обстеженні» [6; 7]. Пацієнт має право на таємницю інформації про стан свого здоров’я та діагноз, який йому встановлено при обстеженні (передбачено Основами законодавства України про охорону здоров’я (ст. 6) та Цивільним кодексом України (ст. 285). Тобто медичний працівник має право розголошувати медичну інформацію тільки за умови отримання згоди пацієнта, її законних представників та в інших випадках, передбачених вітчизняним законодавством.

На думку А.С. Дворніченко, одним із основних завдань у напрямі до європейської інтеграції системи охорони здоров’я України є закріплення і впровадження європейських принципів в законодавство України, яке регулює права пацієнтів, а саме право на медичну таємницю [8].

Взірцем демократичних засад щодо поваги до прав та законних інтересів громадян, у тому числі і у частині, що стосується приватності медичної інформації, є Сполучені Штати Америки (далі – США). Правовий захист у США медичної інформації, яка відноситься до чутливої категорії персональних даних, передбачає

більший рівень захисту, ніж інші категорії персональних даних. Даний напрям регламентовано Законом США про мобільність та підзвітність медичного страхування (Health insurance portability and accountability act або HIPAA), прийнятим у 1996 році. HIPAA – закон, який врегульовує мобільність та підзвітність медичного страхування і встановлює стандарти захисту медичної звітності та особистих медичних даних пацієнтів. Він визначає, які дані пацієнтів захищаються, а також хто повинен дотримуватись вимог HIPAA при роботі з відповідною інформацією. HIPAA відносить до такої інформації: минулі та актуальні дані про стан здоров'я особи (зокрема, анамнез особи, її діагноз, результати проведених медичних досліджень, призначене лікування); дані про надання медичних послуг особі; минулі та актуальні дані про оплату наданих медичних послуг, які надають можливість ідентифікувати особу, або ж є достатня підстава вважати, що особу можна ідентифікувати за такими даними. Варто зазначити, що дані про особу, за якими зазвичай її ідентифікують (місце проживання, ім'я та прізвище, податковий номер тощо) не є такою інформацією та не охоплюються HIPAA. Однак, якщо поруч з такими даними є інформація про стан здоров'я чи надання медичних послуг, то в сукупності такі дані становитимуть відповідну інформацію, яка охоплюється HIPAA. Збір, обробку та захист такої інформації здійснюють визначені юридичні особи (в цілях надання медичних послуг – лікарі та страхові компанії), а також їх бізнес-партнери (особи, які виконують певні функції від імені визначених юридичних осіб або надають їм послуги, що включає в себе використання чи розкриття даної інформації – компанії, які надають послуги з розрахунку вартості медичних послуг та надсилають запити в страхові компанії для отримання оплати за надані медичні послуги) [9].

Таким чином, захист прав людини, в тому числі права на інформацію, є основним конституційним правом. Досить слушною з цього приводу є думка О.Г. Марценюка, відповідно до якої саме забезпечення права людини, в тому числі на медичну інформацію, визначає як рівень демократичності самої держави, так і рівень інтеграції національного права у світове співтовариство, відповідність права міжнародно-правовим стандартам [10].

Література:

1.Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України (ВВР*). 2010. № 34. Ст. 481.

2.Блінова Г.О. Інформаційна приватність у медичній сфері. *Юридичний вісник*. 2014. № 3. С.136–141.

3.Науково-практичний коментар Кримінального кодексу України /за ред. М.І. Мельника, М.І. Хавронюка. 4-те вид., переробл. та допов. К.: Юрид. думка, 2007. 1184 с.

4.Стеценко С.Г., Шатковська І.В. Медичне право України (правове забезпечення лікарської таємниці): монографія. К.: Атіка, 2010. 144 с.

5.Конституція України від 28 червня 1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 43.

6.Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № 40. Ст. 356.

7.Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 р. № 2801-XII. *Відомості Верховної Ради України*. 1993. № 4. Ст. 19.

8.Дворніченко А.С. Правові підстави та умови регулювання розголошення медичної таємниці. *Юридичний часопис Національної академії внутрішніх справ.* 2014. № 2. С. 174–184. С. 176.

9.Захист медичних даних пацієнтів США. URL: https://everlegal.ua/hipaa-yak-zakhyschayut-medychni-dani-patsientiv-v-ssha.

10. Марценюк О.Г. Права фізичних і юридичних осіб на медичну конфіденційну інформацію. *Медичне право України: правовий статус пацієнтів України та його законодавче забезпечення:* матеріали II Всеукраїнської конференції (м. Львів, 17–18 квітня 2008 р.) С. 166–171.

Послявський Денис

ІСЗЗІ, КПІ ім. Ігоря Сікорського,

Сторчак Антон

к.т.н., ІСЗЗІ, КПІ ім. Ігоря Сікорського

ЗАВДАННЯ РОЗПОДІЛУ ВІДПОВІДАЛЬНОСТІ ПРИ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект та особливості його застосування кожного дня привертають все більше уваги вітчизняних та міжнародних науковців. Аналіз наукових робіт [1-7] показав, що серед більшості сучасних технологій цифрової трансформації суспільства саме технологія штучного інтелекту (ШІ) має всі шанси змінити наше життя: зробити його простішим, ефективнішим та збільшити продуктивність, зменшивши при цьому витрати часу. Розвиток ШІ на сучасному етапі цифровізації країни актуалізує завдання регулювання відповідного правового забезпечення.

Зараз штучний інтелект використовується майже в усіх сферах суспільного життя: від потужних діагностичних алгоритмів до точно налаштованих хірургічних роботів в сфері медицини, від налаштування та управління “розумним” будинком до повідомлення останніх новин в залежності від категорії присутніх осіб в повсякденному житті, для потреб армії та поліції створюються нові робот та дрони у сфері оборони, в системах безпеки впроваджуються біометричні можливості. ШІ здатний замінити велику кількість робочих місць, тому що роботи, побудовані на його основі, швидші, ефективніші та дешевші за людей. Під ШІ розумітимемо інтелектуальну систему, що здатна виконувати творчі функції зі здобування, обробки та застосування знань та вмінь, які властиві лише людині [3, с. 2]. Сьогодні виділяють наступну класифікацію ШІ:

– “слабкий штучний інтелект” (WAI – Weak Artificial Intelligence), “вузький штучний інтелект” або “обмежений штучний інтелект” (NAI – Artificial Narrow Intelligence) [4, с. 8] – ШІ, орієнтований на вирішення одного чи декількох завдань, які виконує або може виконувати людина. Слабкий ШІ також називають прикладним штучним інтелектом (AAI – Applied Artificial Intelligence);

– “сильний штучний інтелект” (ASI – Strong Artificial Intelligence), загальний ШІ (AGI – Artificial General Intelligence) – це ШІ, орієнтований на вирішення всіх завдань, які виконує або може виконувати людина [5, с. 5];

– “штучний суперінтелект” (ASI – Artificial Superintelligence) – інтелект, який набагато розумніший, ніж кращій людський інтелект майже в кожній області, в томі числі наукова творчість, загальна мудрість, соціальні навички [6, с. 15].

Застосування технологій ШІ окремо і впровадження технологій Інтернету речей загалом створює новий інформаційно-технологічний простір, в якому вже частково забезпечується потреби людини. Саме том виникає необхідність у створенні правового регулювання функціонування та роботи такого середовища, в якому будуть визначені суспільно-правові відносини між людьми, між людьми та роботами або окремо між роботами.

На ряду із усіма перевагами застосування ШІ в сучасних автоматизованих та інформаційних системах постає питання безпечності застосування ШІ у сферах соціального життя. В [7, с. 25] детально представлено реалізації в робототехніці автономних та когнітивних функцій, що властиві лише людині: здатність вчитися на досвіді, приймати рішення, об’єктивно оцінювати ситуацію. Ці функції фізичної особи можуть спонукати власників ШІ до деструктивних дій, що матимуть шкідливі наслідки та за які, за аналогією до людини, повинна наступати юридична відповідальність. Що стосується неавтономних або частково автономних роботів, то

відповідальність за їх дії та здійснені правопорушення повинна покладатися на власника, розробника та користувача, але це питання поки є невизначеним.

Тому виникає необхідність врегулювання суспільно-правових відносин зважаючи на особливості реалізації роботів в усіх сферах життя. Нормативні акти України не визначають робота, навіть із дуже розвинутим ШІ, суб'єктом правовідносин, оскільки робот не є фізичною або юридичною особою та не здатен виконувати юридичні обов'язки. Натомість в Європейському парламенті запропоновано створення системи реєстрації роботів та сформульовано поняття "електронної особи", яке можливо розглядати, як суб'єкт права, оскільки "електронна особа" є сукупністю юридичних обов'язків і прав, змістом яких можуть визнаватися і дії ШІ [8]. Тобто "електронна особа" є носієм ШІ, що володіє розумом, аналогічним людському, здатністю приймати усвідомлені та не засновані на закладеному творцем такого робота алгоритмі рішення і через це наділеного певними правами й обов'язками. Статус "електронна особа" слід застосовувати, коли роботи самостійно приймають вольові рішення або будь-яким іншим чином взаємодіють з третіми особами [9].

Таким чином, зважаючи на стрімкий розвиток цифрової трансформації держави, доцільно розглянути можливість створення сучасних правових регуляторів у сфері робототехніки та ШІ, спираючись на міжнародний досвід та розроблені європейські правові стандарти, що сприятиме розвитку технології ШІ та забезпечить дотримання прав людини у відносинах з автономними пристроями.

Література:

1. Еннан Р. Є. Правове регулювання відносин у мережі Інтернет. ІТ ПРАВО: Проблеми і перспективи розвитку в Україні: зб. матеріалів наук.-практ. конф., 17 листоп. 2017 р. Львів: НУ «Львівська політехніка», 2017. URL: http://aphd.ua/publication-173/ (дата звернення: 24.04.2021).

2. Карчевський М. В. Основні проблеми правового регулювання соціалізації штучного інтелекту. ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів ІІ-ї Міжнародної науково-практичної конференції. 17 листопада 2017 р. Львів : НУ «Львівська політехніка», 2017. URL: http://aphd.ua/ publication-369/ (дата звернення: 26.04.2021).

3. Штучний інтелект – ефективна та одночасно небезпечна технологія. Чи усвідомлюють суспільство та бізнес ризики та переваги AI? Аналітика Everest-AI-Review. 2019. № 4. URL: https://www.everest.ua/wp-content/uploads/2019/01/Everest-AIReview-%E2%84%965.pdf (дата звернення: 23.04.2021).

4. Agnese Smith. Artificial intelligence. 2015. URL: http://nationalmagazine.ca/Articles/FallIssue2015/Artificialintelligence.asx (дата звернення: 26.04.2021).
5. B.J. Copeland. Artificial intelligence. 2017. URL: https://www.britannica.com/technology/artificial-intelligence (дата звернення: 17.04.2021).
6. Nick Bostrom. How long before superintelligence? Oxfrord Future of Humanity Institute. University of Oxford. Originally published in Int. Jour. of Future Studies. 1998. URL: https://nickbostrom.com/superintelligence.html (дата звернення: 20.04.2021).
7. Mady Delvaux. REPORT with recommendations to the Commission on Civil Law Rules on Roboticshttps. URL: https://www.europarl.europa.eu/ doceo/document/A-8-2017-0005_EN.html (дата звернення: 16.04.2021).
8. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL). URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (дата звернення: 25.04.2021).
9. Штучний інтелект для України – ризик чи можливість. Аналітика Everest-AI-Review. 2018. URL: https://www.everest.ua/wp-content/uploads/2019/01/Everest-AI-Review-%E2%84%965.pdf (дата звернення: 19.04.2021).

Томик Вікторія
Студентка, КПІ ім. Ігоря Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

Розповсюдження та кількість користувачів мережі Інтернет лише зростають з кожним днем, вдосконалюються процеси, які відбуваються у цьому середовищі, збільшується кількість суспільних відносин, які потребують регулювання. Науково-технічний прогрес є каталізатором розвитку інформаційного суспільства, що включає глобалізацію комунікаційних систем, збільшення кола послуг, сервісного простору, клієнтського навантаження. Це стосується і хмарних технологій. Підприємства, установи та організації різних форм власності завзято освоюють їх з метою підвищення ефективності без шкоди для своєї продуктивності у сфері вдосконалення бізнесу, надання освітніх послуг, здійснення управління тощо. Під час вирішення питання щодо запровадження хмарних технологій на тому чи іншому

підприємстві одним з основних завдань є підбір відповідного сервісу, зважаючи на певні правові та технічні фактори, адже водночас з неоспорюваними перевагами даних технологій є і певні ризики, що насамперед стосуються інформаційної безпеки та захисту персональних даних.

Відповідно до визначення, наданого Національним інститутом стандартів і технологій (NIST) хмарними технологіями є така модель, що забезпечує повсюдний та комфортний доступ на вимогу через мережу до пулу обчислювальних ресурсів, що опрацьовуються та оперативно надаються з якомога меншими управлінськими витратами чи необхідністю звернень до провайдера [1, с. 2]. Зокрема сутність цих технологій полягає в тому, що вони дають змогу замінити особам, які їх використовують, свою власну інформаційну структуру, програмне забезпечення чи обчислювальну техніку на послуги провайдерів хмарних систем та отримати при цьому доступ до інформації, мереж чи сервісів з будь-якої точки світу і в будь-який час. Саме це інколи призводить до проблем, пов’язаних з інформаційною безпекою.

Такими напрямками, які викликають найбільше запитань у сфері захисту персональних даних у поєднанні з використанням хмарних технологій є:

- можливість цих сервісів забезпечити зберігання й опрацювання даних відповідно до вимог законодавства;

- гарантування доступу особи, яка використовує хмарні технології, до своїх персональних даних, враховуючи, що вона фактично не здійснює контроль за цим доступом;

- транскордонне пересилання та фізичне розміщення даних, які вносяться особою, оскільки дата-центр, у якому здійснюється опрацювання інформації, знаходиться там, де це вигідно провайдеру, а не користувачу хмарних технологій [2, с.1].

Розв’язання цих та інших проблем можливе з використанням вже наявних або покращених з часом методів криптографічного захисту даних, укладанням договір про надання відповідних послуг з визначенням прав та обов’язків клієнта та постачальника, засобів захисту, які вони повинні використовувати, а також вдосконаленням як міжнародної, так і національної правової бази, що повинна встановлювати основні стандарти та вимоги до хмарних технологій.

До ключових аспектів використання хмарних технологій, які слід врегульовувати у законодавстві, зокрема належать питання конфіденційності, цілісності отриманих персональних даних, їх місцезнаходження та передачі, визначення кола осіб, які ними володіють, захист даних після закінчення договору та відповідальність за надані послуги з боку їх провайдера чи отримувача, можлива

стандартизація, сертифікація цих послуг, контроль з боку держави та заходи щодо сприяння розвитку IT-компаній, які їх надають [3, с. 41].

Деякі керівні принципи опрацювання даних з використанням хмарних технологій, розроблені у країнах Європейського Союзу, закріплені й в законодавстві України. Так Закон України «Про інформацію» встановлює неможливість здійснення без згоди на це особи збору, зберігання, використання чи поширення конфіденційної інформації про неї [4, ст. 11]. А вимоги до обробки персональних даних встановлюються Законом України «Про захист персональних даних». Відповідно до ст. 9 цього Закону опрацювання такої інформації повинно здійснюватися відкрито та прозоро [5, ст. 9].

Прозорість у контексті використання хмарних технологій повинна означати можливість їх користувача оцінити умови використання цієї системи, володіти вільним доступом до відомостей про сам факт і мету зібрання персональних даних, про всіх суб'єктів, які долучаються до їх опрацювання, про місцезнаходження тих технічних засобів, які виконують такі дії, про підстави та порядок настання відповідальності у зв'язку з невиконанням обов'язків, визначених договором, а також про послідовність тих угод, які формуються під час залучення провайдером співвиконавців для здійснення надання хмарних послуг тощо.

Задля забезпечення цього положення такі науковці як Новицький та Дяковський висувають пропозицію щодо запровадження на законодавчому рівні обов'язкової реєстрації суб'єктів, які здійснюють обробку персональних даних, та створення Єдиного державного реєстру баз персональних даних [6, с. 180].

Використання хмарних технологій також повинно включати можливість їх користувачів управляти персональними даними, що знаходяться в обробці, зокрема змінювати, видаляти, блокувати їх. Особливо складним є здатність у зв'язку з відсутністю стандартних форматів даних та процесів сумісності між різними інформаційними системами передати такі персональні дані іншому провайдеру, якщо користувач бажає його змінити. Акцент в даному випадку при гарантуванні прав користувача зроблений на так зване «право бути забутим», що передбачає повне видалення усіх персональних даних після закінчення використання хмарних технологій [7, с. 2026]. Якщо повне видалення цих даних неможливе відповідно до законодавства (наприклад, податкового), то повинно здійснюватися їх остаточне блокування.

Ще одним аспектом використання хмарних технологій є їх географічна віддаленість від користувачів, оскільки розміщення дата-центрів здійснюється на розсуд провайдера і досить часто у країнах з недосконалим законодавством або низьким рівнем захисту персональних даних. А тому ці послуги ще потребують

врегулювання з цього питання з метою уніфікації захисту персональних даних незалежно від юрисдикції, в якій перебуває провайдер.

Отже, хмарні технології не регулюється спеціальним законодавством в Україні, а нормативна база дещо відстає від розвитку ІТ-технологій. Провайдер хмарних послуг несе відповідальність за забезпечення конфіденційності персональних даних у межах Закону України «Про захист персональних даних» з урахуванням особливостей хмарних технологій. Регулювання відносин між особою, що надає ці послуги, та користувачем здійснюється на договірних засадах, оскільки в національному законодавстві відсутні стандарти, які б встановлювали вимоги до якості та надійності хмарних технологій. А тому нормативна база України потребує суттєвих доповнень та вдосконалень у сфері надання ІТ-послуг.

Література:

1. Mell P., Grance T. The NIST Definition of Cloud Computing (Special Publication 800-145): Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology, U.S. Department of Commerce. September 2011. 7 P.

2. Актуальні питання захисту персональних даних у віртуальному середовищі (на прикладі технологій та сервісів «хмарного» обчислення): аналіт. зап. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/aktualni-pitannya-zakhistu-personalnikh-danikh-u-virtualnomu (дата звернення: 24.04.2020).

3. Каріченський О.В. Досвід та переваги використання технологій хмарних обчислень у державних проектах : матеріали Міжнар. наук. конгресу «Інформаційне суспільство в Україні». Київ. 2013 р. С. 41-42.

4. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України.* 1992. № 48, ст. 650.

5. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України.* 2010 р. № 34, ст. 481.

6. Новицький А., Дяковський О. Правове регулювання інформаційних баз

даних, що містять персональні дані. *Підприємство, господарство і право. Інформаційне право.*2017 р. № 10. с. 117-181.

7. Скриньковський Р., Сопільник Р., Малашко О., Віконський В., Ковалів М., Процюк Т., Єсімов С., Заяць Р. Принципи правового регулювання хмарних технологій для обробки персональних даних. *Траєкторія науки. Право і безпека.*2019 р. № 7. с. 2022-2029.

Секція № 2

Тімашов Віктор
д.ю.н., професор
Ніколаєва Людмила
к.ю.н., професор
Дем'яненко Едуард
Київський національний
торговельно-економічний університет

ПРОБЛЕМИ ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ В СФЕРІ ОХОРОНИ ЗДОРОВ'Я

За сучасних умов розвитку інформаційних технологій відзначається автоматизація процесів усіх галузей економіки. Адже саме під впливом ІТ відбувається повноцінна модернізація усіх процес підприємства, зокрема автоматизація управлінських процесів, що призводить до формування ефективних управлінських рішень та роблять адміністративні процес більш зрозумілими та простими. Технологія Інтернету речей (далі- IoT) зазнає активного використання на багатьох підприємствах, зокрема у медичних установах. Використання зазначених технологій є необхідною передумовою для розвитку сфери охорони здоров'я.

Проте на чолі із переваги, які отримують медичні установи від IoT відзначаються і недоліки їх впровадження: ризик неправомірного використання; збір персональних даних громадян, що призводить до втручання в особисте життя.

«Інтернет речей» (Internet of Things) – мережа, у якій відбувається взаємодія усіх компонентів між собою, які суспільство використовує у повсякденному житті. Під час обміну інформацією, так звані «речі» встановлюють контакт між собою. Даний процес називається комунікацією «речей», які взаємодіють між собою та зовнішнім середовищем. При цьому вони передбачають виконання певних дій без участі людини у процесі. Отже, IoT є комплексом взаємопов'язаних між собою механічних та цифрових пристроїв, об'єктів або людей, які мають специфічні ідентифікатори та можливість передавати інформацію по мережі, не вимагаючи від людини взаємодії з іншою або людини з комп'ютером [1].

Таким чином, IoT є концепцією, яка дає змогу реалізувати ряд електронних технологій, зокрема таких як-от: медичні програми за допомогою підключення до інтернету та спеціального програмного забезпечення можуть збирати та аналізувати необхідну інформацію, надавати віддалену допомогу пацієнтам, розпізнавати

симптоми та протікання хвороби та здійснювати повноцінний контроль за станом пацієнта та його лікуванням.

Проте поряд із переваги впровадження IoT у сферу охорони здоров’я можна виокремити і ряд проблем щодо безпеки та конфіденційності. Така ситуація зумовлена тим, що у процесі використання IoT поєднується багато пристроїв між собою за допомогою інтернету і використовується багато точок доступну, які мають бути якісно захищеними. Шахраї можуть отримати доступ до мережі використовуючи недостатньо захищені IP-пристрої. Внаслідок того, що усі пристрої взаємопов’язані між собою, для порушення системи та витоку даних достатньо пошкодити лише один компонент [1].

У сфері охорони здоров’я приділяють значну увагу використанню IoT, адже керівники усвідомлюють, що у їх використанні покладено великий потенціал, який здатен покращити та оптимізувати діяльність медичних установ.

На сьогодні, IoT є одними із найсильніших мотиваційних факторів для інноваційного розвитку новітніх цифрових технологій, електроніки, автоматизації управлінських процесів. Проте активне поширення IT у сфері охорони здоров’я може призвести до зростання кіберризиків та проблем із кібер безпекою на підприємствах [2].

У разі використання IoT у медичних закладах відкриваються нові можливості для кібератак. У такому випадку, IoT створюють як зручність для закладу, так і високий рівень відповідальності за збереження персональної інформації користувачів.

Ще однією проблемою, яка виникаю із впровадження IoT у діяльність підприємства є ситуації, коли розробники залишають незадокументований канал, на якому збираються дані щодо використання пристроїв, але дають змогу отримати персональні дані пацієнтів.

Може поширитися проблема шкідливості внаслідок використання сигналу 4G та 5G. За даними вчених оцінити безпеку сигналу 4G при існуючих методиках виміру практично неможливо.

Проте, масштабне використання IoT може призвести до подальшої ідентифікації нових проблем та ризиків щодо якісної безпеки персональної інформації. У такому випадку, відзначаються труднощі у збереженні конфіденційності лікарських даних.

Найбільшу роль у проблемній групі відіграє правове регулювання використання IoT, які зумовлені тим, що впровадження новітніх технологій базується на використання IT та IP технологій. Насамперед, це пов’язано із створенням та реалізацією правових відносин у процесі використання IP технологій

та штучного інтелекту, а також правових механізмів регулювання інфраструктурної безпеки впровадження та використання технологій IP [3].

Інтернет речей (Internet of Things) відіграє чималу роль у функціонуванні об’єктів у сфері охорони здоров’я і все більше медичних установ ставлять перед собою завдання впроваджувати IoT у своїй діяльності. Досвідчені керівники стверджують, що інвестиції в автоматизацію процесів займають першочергове місце у довгострокових планах, і є більш пріоритетними, ніж збільшення об’ємів виробництва послуг.

Література:

1. Definition Internet-of-Things-IoT. URL: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.
2. Парамонов В. Інтернет речей. «Розумна» електроніка. URL: https://www.turkaramamotoru.com/uk/Інтернетречей-20010.html
3. «Штучний інтелект», Дмитренко В.І. Смарт-сіті чи електронне місто: сучасні підходи до розуміння впровадження е-урядування на місцевому рівні. Інвестиції: практика та досвід. № 13. 2016. С. 89-93.

Чесницький Данило

Студент, КПІ ім. Ігоря Сікорського

ПРАВОВИЙ СТАТУС НЕВЗАЄМОЗАМІННИХ ТОКЕНІВ (NFT)

За останнє десятиріччя технологія блокчейн стала однією з найпопулярніших тем у контексті інформаційного суспільства. Починаючи з 2012 року інтерес до пошукового запиту «blockchain» виріс у понад 10 разів, а експонентний ріст спостерігається останні 5 років [1]. За цей технологія перестала бути предметом зацікавленості невеликої групи людей та знайшла своє застосування у сфері фінансів, освіти, мистецтва, моди, та юриспруденції. Одним з найбільш гучних проявів технології блокчейн за 2020 рік можна вважати невзаємозамінні токени, так звані «non-fungible tokens» (далі - NFT). Завдяки новій розробці з’явилася можливість здійснювати покупку на продаж унікальних предметів цифрового та реального світу. Однак, одразу з появою новітнього інструменту постало питання правового регулювання технології NFT та всіх суміжних прав, які вона породжує. Наразі дискусія навколо закріплення правового статусу NFT в законодавстві України продовжується, тому доцільно розглянути існуючі позиції.

Для визначення поняття невзаємозамінних токенів необхідно зазначити, що токен, це елемент обліку у блокчейн-системах, завдяки якому можна децентралізовано зберігати інформацію різного типу. Токени поділяються на взаємозамінні та невзаємозамінні. До першого виду відносять криптовалюти Bitcoin, Litecoin, Ethereum тощо. Їх взаємозамінність полягає у повній ідентичності токенів певної криптовалюти між собою. Тобто, один біткойн абсолютна копія іншого біткойну. На відміну від взаємозамінних токенів, кожен NFT унікальний, та містить всю інформацію про цифровий об’єкт (дані цифрового об'єкта, історія операцій, список володільців і т.д.) [2]. Тобто, NFT – це криптовалюта, яка є цифровим аналогом оригінальних речей реального світу.

Поява технології NFT спричинила нові можливості для розвитку торговельних відносин. З 2018 року з’являються майданчики для продажу невзаємозамінних токенів: OpenSea, Foundation, Rarible, SuperRare тощо [3]. Майданчики стали інструментом для використання токенів у всіх сферах цифрової торгівлі, де існує штучний дефіцит. Найбільш поширеними цифровими об’єктами, що піддаються токенізації є цифрові твори мистецтва (статична та динамічна комп’ютерна графіка), відеозаписи, ігрові активи, предмети колекціонування з комп’ютерних ігор та інші цифрові об’єкти, які представляють унікальність завдяки своєму автору, місцю або часу публікації. Одним з останніх та найбільш значущих проявів NFT стала токенізація договірних зобов’язань реального світу [4]. Вище перелічені процеси свідчать про появу нового виду відносин, які мають особливу форму, застосування, а разом з тим породжують права та обов’язки.

Відповідно до Цивільного кодексу України правом інтелектуальної власності є право особи на результат інтелектуальної та творчої діяльності [5]. NFT токен є результатом такої діяльності, тобто, з точки зору закону, може вважатися об’єктом інтелектуальної власності. Кожен NFT токен має автора, у якого є виняткове право на використання свого твору. Також автор може передати своє право повністю або надати часткове право на використання твору. Найбільш поширений спосіб передачі прав — продаж на аукціонах, які проводять NFT-майданчики. Інформація про власника NFT відкрито зберігається у блокчейні, і довести права на твір покупець може шляхом пред'явлення свого електронного гаманця, синхронізованого з обраною блокчейн-платформою, в який NFT потрапить за підсумками угоди [3].

Проте, попри те, що NFT є об’єктом інтелектуальної власності, перспективи захисту гіпотетично порушеного права у судовому порядку низькі. Вважаємо, що зазначена проблема спричинена декількома чинниками:

1. Ліцензійні угоди майданчиків з продажу невзаємозамінних токенів не передбачають передачу виключних прав від автора до покупця. Покупець токена набуває лише цифрове право власності;
2. Через небажання майданчиків брати відповідальність за врегулювання майнових та немайнових прав сторін, до покупця перейдуть тільки ті права, які прямо вказані в окремому договорі з правовласником, звісно якщо такий існує;
3. Судова практика стосовно справ, пов'язаних з блокчейном вкрай мала, стосовно більш вузькопрофільного NFT взагалі відсутня;
4. Відсутність нормативно-правового визначення статусу NFT-токенів у європейському законодавстві, та, зокрема, в законодавстві України.

Вірогідно, що майданчики з продажу NFT-токенів надають автономність сторонам у визначенні переліку прав, які переходять до автора до покупця та можливі варіанти використання придбаного контенту. Більш того, директор міжнародної криптобіржі CEX.IO Дмитро Волков вважає, що розвиток технології NFT продовжується і зарано узаконювати технологію, яка може знайти свій прояв у сфері інтернету речей («розумні» речі, право володіння якими підтверджується невзаємозамінним токеном), реєстрації патентів та компаній, дистрибуції продуктів, які потребують ідентифікації [6]. На нашу думку, технологія NFT дійсно перспективна і перебуває у стані активного розвитку, однак це не виключає необхідності її законодавчого врегулювання.

Підтвердженням необхідності врегулювання технології блокчейн і, зокрема, NFT є законопроєкт №3637 «Про віртуальні активи», який готується на друге читання у Верховній Раді [7]. Одним з ініціаторів розробки проєкту закону стало Міністерство цифрової трансформації України. Відповідно до позиції Міністерства законодавчо врегульований правовий статус віртуальних активів надасть юридичний захист користувачам та учасникам ринку. Ухвалення законопроєкту "Про віртуальні активи" дозволить прибрати ризики для українського криптобізнесу, а власникам криптовалют — не тільки декларувати власні доходи у віртуальних активах, але й захистити набуті права [8].

З точкою зору Міністерства згодні і юристи, наприклад Христина Цимбалюк з юридичної фірми Eterna Law наголошує, що без законодавчого врегулювання NFT та ринку криптовалют в цілому, об'єкти та учасники ринку криптовалют знаходяться поза правовим полем держави. Юристи компанії Alcor Оксана Петрусь і Аліна Зорченко вважають, що з урахуванням чинного законодавства найлогічніше було б віднести NFT до товару, зокрема — до нематеріальних активів. В цьому випадку при операції купівлі-продажу оподаткування повинно виникати тільки на

стороні продавця. Дещо відмінною є думка керуючого партнера Juscutum Артема Афяна. На його думку, NFT варто розглядати як предмет мистецтва і продавати за правилами, які відповідають цьому поняттю, однак без змін до законодавства використовувати цей підхід зарано [9]. Загалом, юридична спільнота слідкує за зростаючим інтересом суспільства до NFT та багатомільйонними операціями з їх продажу. В наявній ситуації логічним є інтерес податкових служб та законодавців до ринку криптовалют.

Таким чином, для законодавчого закріплення правового статусу невзаємозамінних токенів на національному рівні необхідністю стають наступні кроки:

1. Постійний моніторинг технології NFT та ринку криптовалют для запровадження та оновлення нормативно-правової бази;
2. Впровадження м'якої податкової політики для мінімізації тіньового сектору ринку криптовалют,
3. Запуск освітньої програми по інформуванню населення, особливо представників творчих професій про можливості технології NFT та блокчейн.

У підсумку, можна стверджувати, що технологія NFT знаходиться у початковій стадії свого розвитку, однак вже породжує відносини, які повинні бути законодавчо врегульовані. Держава займається розробкою нормативно-правової бази для регулювання ринку криптовалют, що є показовим у прагненні України побудувати інформаційне суспільство, адже тема блокчейну та похідних від нього явищ є відкритою у всьому світі.

Література:

1. «blockchain» // Google Trends: [Веб-сайт]. URL: https://trends.google.com/trends/explore?date=2007-04-03%202017-05-03&q=blockchain (дата звернення: 27.04.2021).
2. Що таке NFT і чому всі про це говорять? // Tokar.ua: [Веб-сайт]. URL: https://tokar.ua/read/44528 (дата звернення: 27.04.2021).
3. Правові аспекти NFT // vc.ru: [Веб-сайт]. URL: https://vc.ru/legal/220843-pravovye-aspekty-nft-pochemu-vypiska-iz-egryul-eto-schitay-chto-nft-no-ne-sovsem (дата звернення: 27.04.2021).
4. Сизоненко В. Токенізація активів – реалії та можливості // Юргазета: [Веб-сайт]. URL: https://yurgazeta.com/publications/practice/informaciyne-pravo telekomunikaciyi/tokenizaciyaaktiviv--realiyi-ta-mozhlivosti (дата звернення: 27.04.2021).

5. П.2 ст. 418 Цивільний Кодекс України від 16.01.2003р. №435-IV. Дата оновлення: 01.01.2021. URL: https://zakon.rada.gov.ua/laws/show/435-15#n2235 (дата звернення: 27.04.2021).

6. Степанова Ю. После просмотра сжечь. *Тематическое приложение к газете «Коммерсантъ»*. Москва, 2021. № 55. С. 18.

7. Проект Закону про віртуальні активи: веб-сайт. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110 (дата звернення: 27.04.2021).

8. Розвінчуємо міфи про законопроєкт «Про віртуальні активи»// Прес-офіс Комітету цифрової трансформації України: [Веб-сайт]. URL: https://thedigital.gov.ua/news/rozvinchuemo-mifi-pro-zakonoproekt-pro-virtualni-aktivi (дата звернення: 27.04.2021).

9. Нужно ли платить налоги с NFT-сделок? Сравниваем кейсы США, России и Украины // forklog: [Веб-сайт]. URL: https://forklog.com/nuzhno-li-platit-nalogi-s-nft-sdelok-sravnivaem-kejsy-ssha-rossii-i-ukrainy/ (дата звернення: 27.04.2021).

Чорнобай Евеліна

студентка, КПІ ім. Ігоря Сікорського
Науковий керівник: Сергій ДОРОГИХ,
к. ю. н., старший науковий співробітник
ДНУ «Інститут інформації, безпеки і права
НАПрН України», старший викладач
КПІ ім. Ігоря Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В ДЕРЖАВНОМУ СЕКТОРІ УКРАЇНИ

В епоху глобальної цифровізації забезпечення максимального розвитку та впровадження передових інформаційних технологій є запорукою стабільного та ефективного функціонування будь-якої держави. Саме тому міністерства, відомства та інші офіційні державні структури США, Великої Британії, країн ЄС та Південно-Східної Азії в рамках реалізації Стратегії Cloud First вже багато років у своїй діяльності активно застосовують *хмарні технології*. За умови розумного впровадження і використання хмарні технології надають масу переваг, серед яких – зниження загальної вартості утримання ІТ-інфраструктури, зростання ефективності використання державних ресурсів, підвищення якості надання послуг тощо.

Україна, наразі, істотно відстає від світових тенденцій, але очевидним є той факт, що скоро нашим державним органам доведеться переймати такий світовий досвід.

Довгий час про впровадження хмарних технологій в Україні навіть не йшлося. Однак, у червні 2020 року Верховна Рада України прийняла за основу Проєкт Закону України «Про хмарні технології» (№2655 від 20.12.2019), чим заклала підґрунтя для правового регулювання вказаної сфери технологій та переходу державного сектору на застосування хмарних технологій. Наразі ж, законопроєкт готується до другого читання, що надає нам змогу проаналізувати запропоновані норми і виокремити основні переваги та недоліки в запропонованому правовому регулюванні вказаної сфери.

Перше, на що хотілося б звернути увагу, аналізуючи проєкт закону – це те, наскільки «поверхнево» ним врегульовані питання, пов’язані з практичним застосуванням хмарних технологій. Зокрема, законопроєкт не визначає основні вимоги до регулювання надання хмарних послуг, не визначено специфіку захисту споживачів хмарних послуг, а також не врегульовує питання надання хмарних послуг у приватній сфері, не зважаючи на те, що відповідно до статті 1 він регулює відносини, які виникають при наданні хмарних послуг, тобто усім можливим користувачам.

Враховуючи те, що законопроєкт фактично є першою спробою запровадження використання органами державної влади у своїй діяльності хмарних технологій, на мою думку, вже на етапі розробки законопроєкту слід було б деталізувати та розширити його норми задля уникнення можливих непорозумінь, попередження та захисту від незаконних посягань та зловживань переданими на хмари масиви даних внаслідок відсутності правозастосовчої практики у сфері хмарних технологій.

Законопроєктом передбачено, що серед учасників відносин у сфері хмарних послуг є особи, майно або послуги яких використовують надавачі хмарних послуг або надавачі супутніх послуг для надання послуг [1]. При цьому, не деталізовано, яким вимогам мають відповідати такі особи, як, з якою метою та за яких умов вони залучатимуться до реалізації положень вказаного закону та яку відповідальність нестимуть у разі порушення його вимог.

Державне регулювання надання хмарних послуг, згідно проєкту, здійснює, зокрема, уповноважений орган, який визначається Кабінетом Міністрів України [1]. Водночас незрозуміло, чи це буде новостворений орган, чи вже наявний орган, наприклад, Міністерство цифрової трансформації України. На мою думку, недоцільно було б утворювати новий орган для регулювання відносин у сфері хмарних послуг, враховуючи те, що масив повноважень, відведений йому законопроєктом, досить невеликий.

Основний акцент проєкту відведено підзаконним нормативно-правовим актам та договірним конструкціям, які будуть необхідним для реалізації положень цього закону. Тобто законопроєкт встановлює лише загальні правові норми у сфері надання хмарних послуг, «перекладаючи» основний масив деталізації таких відносин «на плечі» розроблених та затверджених Кабінетом Міністрів України порядків, постанов та укладених між публічними користувачами та надавачами хмарних послуг договорів.

Попри те, що автори законопроєкту визначили одним із його переваг оптимізацію витрат, пов’язаних з утримання органів влади, що, як наслідок, призведе до зменшення корупції, аналізуючи проєкт закону, можна знайти низку положень, які потенційно несуть в собі певні корупційні ризики.

Зокрема, проєктом не передбачено вичерпного переліку вимог для включення чи виключення надавача хмарних послуг до Переліку надавачів хмарних послуг, передбачено невичерпний перелік документів, які будуть необхідними для подачі надавачами хмарних послуг для їх включення до Переліку, що потенційно може призвести до зловживань посадових осіб Уповноваженого органу.

Надзвичайно важливим є питання інформаційної безпеки у сфері надання хмарних послуг, яке законопроєктом не деталізоване. Оскільки надання хмарних послуг територіально не обмежене, то можливим є виток інформації з обмеженим доступом за межі держави, що може становити загрозу для національних інтересів.

Окремо потребує уваги питання, пов’язане з притягненням до відповідальності у разі порушення норм законодавства у цій сфері.

Законопроєктом не врегульовано питання відповідальності надавача хмарних послуг та публічного користувача у разі порушення вимог законодавства у сфері надання хмарних послуг. Зокрема, проєкт закону передбачає можливість виключення надавача хмарних послуг з Переліку в разі отримання інформації про набрання законної сили рішенням суду про виключення надавача хмарних послуг з такого Переліку [1]. Водночас ні чинним законодавством, ні законопроєктом не передбачено, за сукупності яких умов та на якій підставі суд може прийняти таке рішення, адже відсутньою є відповідальність таких надавачів хмарних послуг у сфері надання хмарних послуг, яка б полягала у виключенні з Переліку надавачів хмарних послуг.

Проєкт закону недостатньо чітко регламентує вид, умови та підстави відповідальності надавача хмарних послуг та публічного користувача перед третіми особами, а також обсяг юридичної відповідальності кожного з учасників відповідних правовідносин.

Таким чином, у разі виникнення внутрішніх та зовнішніх загроз, здійснення кібератак, незрозуміло, яким чином захищатимуться порушені права таких третіх осіб та яка відповідальність наставатиме для надавачів хмарних послуг та публічних користувачів внаслідок настання таких загроз.

Договором про надання хмарних послуг передбачено, що однією з його істотних умов є питання захисту даних (зокрема персональних) при наданні хмарних послуг та порядок захисту від несанкціонованих дій. При цьому публічний користувач та надавач хмарних послуг несуть субсидіарну відповідальність за зобов'язаннями при виконанні договорів при наданні хмарних послуг в частині забезпечення кібербезпеки. Зазначене перекладає відповідальність за захист даних в системі хмарних обчислень безпосередньо на розсуд користувача та надавача хмарних послуг, що не є обґрунтованим, зокрема, в частині надання хмарних послуг публічним користувачам.

Підсумовуючи, слід зазначити, що запровадження в Україні хмарних технологій є важливим етапом з переходу від архаїчності до новацій у вигляді цифровізації та діджиталізації, які є неминучими та необхідність яких є очевидною. Саме законопроєкт України «Про хмарні послуги» став показником реальної політики змін в інноваційному секторі економіки та правовідносин, своєрідним «пусковим важелем» зі скорочення бюджетних витрат, залучення інвестицій для розвитку бізнесу та скорочення цифрового розриву з передовими країнами світу.

Однак, на мою думку, під час підготовки проєкту Закону України «Про хмарні послуги» до другого читання, законодавцю слід більш ґрунтовно деталізувати положення закону, зокрема ті, що пов'язані з організацією та державним регулюванням сфери надання хмарних послуг, визначенням вичерпного переліку конкретних вимог до надавачів хмарних послуг, зокрема, з міркувань безпеки, та документів, які ними подаються, передбаченням запобіжників виникнення загроз для інформаційної та кібербезпеки, а також з детальним визначенням відповідальності публічних користувачів, надавачів хмарних послуг та третіх осіб у випадку порушень законодавства у сфері надання хмарних послуг.

Література:

1. Про хмарні послуги [Електронний ресурс]: проєкт Закону України №2655 від 20.12.2019. Документ не було опубліковано. Доступ із інформ.-правової системи «ЛІГА- ЗАКОН».

Шершньова Анастасія

Студентка, КПІ ім. Ігоря Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН У СФЕРІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ.ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД

Поняття «Штучний інтелект» дедалі частіше можна почути у різних джерелах інформації.Під поняттям штучний інтелект часто розуміють здатність інженерної системи здобувати, обробляти та застосовувати знання та вміння.Яскравим прикладом штучного інтелекту є комп'ютери. Застосування штучного інтелекту є процес активного використання найсучасніших наукових досягнень у сфері інформатики в різноманітних галузях життєдіяльності суспільства.[2]

Штучний інтелект вивчає методи розв'язання завдань, які потребують людського розуміння. Штучний інтелект — це системи, які можуть оперувати зі знаннями, а найголовніше — навчатися.

Основна проблематика даної доповіді:

Відсутність будь-якої нормативно-правової бази в Україні, і досить низька її якість у всьому світі.

Відсутність регулювання правовідносин між штучним інтелектом та людьми.

Відсутність кримінальної відповідальності за порушення закону.

Приблизно з початку двохтисячних років почали відбуватися прогресивні прориви в галузі інтелектуальної власності та права. З часом штучний інтелект поступово почав проникати в різні аспекти правової системи.

Отже, в межах закону можна виділити три категорії суб'єктів правового регулювання штучного інтелекту: 1)адміністратори закону (тобто ті, хто створює та застосовує закон, включаючи державних чиновників, таких як судді, законодавці, адміністративні чиновники та поліція);2) ті, хто використовує штучний інтелект в юридичній практиці, насамперед адвокати);3)ті, хто регулюється законом (тобто люди, підприємства та організації, які регулюються законом і використовують закон для досягнення своїх цілей). [6, с. 12]

Я вважаю ,що застосування штучного інтелекту в праві дуже потрібне, і на разі на міжнародному рівні відбуваються зрушення у цій темі.

Нещодавно Європарламент ухвалив Резолюцію «Норми цивільного права про робототехніку». Документ, що складається з понад сотні пунктів, присвячено найрізноманітнішим аспектам і проблемам робототехніки та штучного інтелекту.[1]

Зокрема, пропонується закріпити правові основи використання штучного інтелекту та впровадження загальноєвропейської системи реєстрації «розумних» машин. За задумом парламентарів, окремим категоріям роботів слід присвоїти індивідуальний реєстраційний номер, який заноситиметься до спеціального реєстру, де можна буде знайти детальну інформацію про робота, включаючи дані про виробника, власника й умови виплати компенсації у разі спричинення шкоди. А підтримкою системи штучного інтелекту та її контролем повинно займатися спеціалізоване агентство з робототехніки, яке могло б взятися і за інші аспекти регулювання у цій області.

Якщо брати до порівняння наше українське законодавство то, на жаль ,вітчизняні закони не регламентують правові основи використання творів, створених без участі людини і автором твору визнає лише фізичну особу. Беручи до прикладу азіатські країни, то в Японії ще у 2016 році на засіданні державної комісії з інтелектуального права було прийнято рішення розпочати розробку нормативних документів щодо захисту авторських прав на продукти творчої діяльності, створені штучним інтелектом.

Штучний інтелект активно використовуються юристами, на сьогодні вже існують юридичні компанії які розробляють, наприклад, програми для прогнозування результату судової справи. Цей напрямок користується попитом та допомагає адвокату у його роботі, як стверджують самі розробники. Вони зараз тестують та опробовують цю систему, її роботу та результати.

Також в Європі вже почалося впровадження штучного інтелекту в судову владу. Зокрема вчені з Університетського коледжу Лондона і Університету Шеффілда створили “комп’ютерного суддю”, який передбачає рішення Європейського суду з прав людини з точністю до 79 %. Розроблений алгоритм бере до уваги не лише законні докази, але й моральний бік справи. “Комп’ютерний суддя” аналізує текст справи, використовуючи «алгоритм машинного навчання”. [7] Науковці не розглядають винахід як заміну суддів чи адвокатів, але вважають його корисним для швидкого виявлення закономірностей у прийнятті рішень суддями. “Це може бути цінним інструментом для визначення справ, у яких є порушення Європейської конвенції про права людини”, – зазначено у повідомленні. Для розробки алгоритму команда дозволила “комп’ютерному судді” просканувати опубліковані рішення з 584 справ щодо катувань, приниження гідності та справедливих суддів: “електронний суддя” встановив вердикти з 79 % точності. Одночасно вчені встановили, що рішення Європейського суду з прав людини часто базуються на моральних аспектах, а не правових аргументах. І тому про повну замінну суддів на штучний інтелект не може йти і мови, адже штучний інтелект ніколи не зможе відчувати і буде опиратись лише на правову сторону справи, без будь-яких моральних принципів.

Все частіше замість поняття “штучний інтелект” почали вживати поняття “робот”. Проаналізувавши деякі наукові роботи вчених-юристів я знайшла декілька дефініцій: 1)простий робот (simple robot) – інтеграція прикладного ШІ і технічної системи, що дозволяє реалізовувати одну або кілька когнітивних функцій людини в процесі здійснення конкретного виду діяльності, пов'язаної, як правило, з однорідними об'єктами, що мають матеріальний або нематеріальний зміст; 2)робот-андроїд (robot android) – інтеграція загального ШІ і технічної системи, що дозволяє реалізовувати безліч когнітивних функцій в процесі здійснення будь-якого виду діяльності без участі людини, пов'язаної з різними об'єктами, що мають матеріальний або нематеріальний зміст; 3)андроїд (android) – інтеграція супер ШІ і технічної системи, що дозволяє реалізувати повну множину когнітивних функцій в процесі здійснення будь-якої раніше відомої або невідомої діяльності без участі людини, пов'язаної з різними відомими або раніше невідомими об'єктами, що мають матеріальний або нематеріальний зміст.[3]

Якщо поглянути на перспективи правового регулювання в умовах застосування і використання штучного інтелекту то, можна виявити наявність трьох основних гіпотез, які власне і визначають основний зміст наукових підходів до вдосконалення або реформування правових систем, що обумовлено використанням роботів: 1)роботи є об'єктом суспільних відносин, а значить і об'єктом правовідносин; 2)роботи є суб'єктом суспільних відносин, а значить можуть бути суб'єктом правовідносин; 3)роботи можуть бути як об'єктом, так і суб'єктом суспільних відносин, а значить можуть бути як об'єктом, так і суб'єктом правовідносин.[5, с. 89]

Дивлячись на такий стрімкий розвиток Науково-технічного прогресу можна навіть припустити ,що в майбутньому можливе наділення штучного інтелекту статусом “електронної особи” в якості учасника суспільних відносин.

В майбутньому наше українське законодавство чекають зміни, адже якщо ми хочемо бути сучасною, демократичною та прогресивною країною то нам потрібно розпочати із нововведень в наше національне законодавство, наприклад потрібно створити закон який би регулював суспіль відносини з приводу застосування та використання штучного інтелекту та внести деякі зміни до кримінального та цивільного законодавства законодавства, зокрема: 1)надати штучному інтелекту статусу «електронної особи»; 2)врегулювати права інтелектуальної власності для текстів, творів, наукових робіт і т. д. що були створенні штучним інтелектом в цивільному законодавстві;3)встановити відповідальність за неправильне або незаконне використання штучного інтелекту яку повинна нести фізична або юридична особа, але ця відповідальність повинна бути точно прописана у нормативно-правовому забезпеченні; 4) захист персональних; 5)регулювання

господарської діяльності з виробництва роботів чи програмного забезпечення. Але однією із найголовніших пропозицій є прийняття єдиного визначення поняття штучного інтелекту для подальшого дослідження та розвитку права в даній сфері суспільних відносин.

Література:

1. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).
URL:http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN
2. Tim Urban. The AI Revolution: The Road to Superintelligence. January 22, 2015. URL: https://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html
3. Vincent C. Müller. Legal vs. ethical obligations – a comment on the EPSRC's principles for robotics. Journal Connection Science, Volume 29, Issue 2: Ethical Principles of Robotics. June 2017, Pages 137-141. URL: http://www.tandfonline.com/doi/full/10.1080/09540091.2016.1276516
4. Баранов О.А. «Інтернет речей» як правовий термін. Юридична Україна. – 2016. – № 5-6. – С. 96-103. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2016_5-6_16.pdf
5. Городиський І.М.(2019) Тенденції розвитку правового регулювання штучного інтелекту в європейському союзі
6. Карчевський М.В. (2017)Правове регулювання соціалізації штучного інтелекту С. 99-108.

Щепеткова Вікторія

Студентка, КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Світ розвивається з кожним днем, а разом з ним й усі сфери нашого життя. Особливо це стосується науково-технічного прогресу, який все більше набирає обертів та зацікавлює суспільство своєї різноманітністю. Проте разом із

позитивними аспектами такого розвитку, зустрічаються й проблеми, які виникають та потребують вирішення. Зокрема, все частіше науковці приділяють увагу питанню правового регулювання штучного інтелекту, даний аспект включає в себе як позитивні, так і негативні моменти.

Поняття “штучний інтелект” почало існувати ще з 1956 року, у стінах Стенфордського університету. Термін «інтелект» (intelligence) походить від латинського поняття intellectus – «розум». [1, С.62] Щодо визначення даного явища, то тучний інтелект (artificial intelligence) розуміється як здатність автоматичних систем брати на себе функції людини вибирати і приймати оптимальні рішення на основі раніше отриманого життєвого досвіду і аналізу зовнішніх впливів. Оксфордський словник, наприклад, пропонує наступне визначення: штучний інтелект – це теорія і розробка комп'ютерних систем, здатних виконувати завдання, які зазвичай вимагають людського інтелекту, таких як візуальне сприйняття, розпізнавання мови, прийняття рішень і переклад між мовами [2]

На мою думку, штучний інтелект - це дуже великий прогрес у технологічній сфері, який може забезпечити людству уникнення багатьох проблем у майбутньому. Адже, він дійсно має багато переваг. Наприклад, його можливості набагато швидші за людські, ручні. Проте, важливо, щоб дане явище було добре висвітлено та врегульовано на законодавчому рівні нашої держави. Чому саме йде мова про Україну? Тому, що у деяких країнах світу штучний інтелект вже впровадився у правову систему. Наприклад провідні європейські держави законодавчо визнають автором твору комп’ютерну програму і готові поставити штучний інтелект на один щабель з людським.

Японія найбільше просунулась у цій сфері. Ще у 2016 р. на засіданні державної комісії з інтелектуального права було прийнято рішення розпочати розробку нормативних документів щодо захисту авторських прав на продукти творчої діяльності, створені штучним інтелектом. А ось українське законодавство доки не регламентує правові основи використання творів, створених без участі людини і автором твору визнає лише фізичну особу. [3]

Також, Європарламент ухвалив Резолюцію «Норми цивільного права про робототехніку». Документ, що складається з понад сотні пунктів, присвячено найрізноманітнішим аспектам і проблемам робототехніки та штучного інтелекту. Зокрема, пропонується закріпити правові основи використання штучного інтелекту та впровадження загальноєвропейської системи реєстрації «розумних» машин.

Проте чинне законодавство України й більшості країн значно відстає від технологічних досягнень і не регулює питання захисту прав інтелектуальної власності на об'єкти, створені штучним інтелектом. Закони України "Про авторське

право і суміжні права", "Про охорону прав на винаходи та корисні моделі" передбачають, що автором є фізична особа, яка своєю творчою працею створила твір, а винахідником – людина, інтелектуальною й творчою діяльністю якої створено винахід.

Наразі наше законодавство пов'язує авторство й створення об'єктів права інтелектуальної власності тільки з людиною, тож у правовому полі комп'ютери, програми та інші форми вираження штучного інтелекту не є авторами й винахідниками. Така ситуація склалася, зокрема, і тому, що штучний інтелект не розглядають як окремий суб'єкт.

Цивільний кодекс України та інші акти цивільного законодавства України не містять поняття “робот”, “штучний інтелект”, у зв’язку з чим для подальшого визначення та конкретизації правового статусу робота як об’єкта правовідносин, необхідно застосовувати за аналогією норми, які стосуються об’єктів цивільних прав, виходячи із дефініцій “робота”, “штучний інтелект”, які містяться в науковій літературі.

Але на мою думку, дана ситуація скоро зміниться. Тому що в умовах сьогодення, не можна ігнорувати такі технологічні процеси, як розвиток та закріплення штучного інтелекту. Зокрема, карта правових реформ використання ШІ в Україні має містити такі напрями:

– цивільне законодавство (визначення правосуб’єктності, зокрема, в яких ситуаціях він може діяти в якості посередника фізичної чи юридичної особи; укладати договори; нести цивільно-правову відповідальність);

– кримінальний закон (визначення кримінальної відповідальності ШІ);

– страхове законодавство;

– антидискримінаційне законодавство (питання рівності людини і осіб, які використовують ШІ; питання з критеріями та даними, які надаються ШІ);

– захист персональних даних (можливості надання диференційованої згоди на обробку персональних даних, а також удосконалення механізму інформованої згоди на обробку персональних даних);

– законодавство у сфері інтелектуальної власності;

– медичне право (використання ШІ у медичній сфері, аспекти діяльності лікаря, який використовує ШІ).[5]

Отже, враховуючи все вищесказане, слід зазначити, що на даному етапі штучний інтелект та його діяльність не врегульована на належному рівні нашим законодавством, як і в більшості країн світу. Проте, нам необхідно йти в ногу з часом, та змінювати це становище, беручи приклад з більшості європейських країн, які стали на шлях технологічного розвитку. Обравши шлях закріплення штучного

інтелекту на законодавчому рівні ми зможемо вийти на новий етап освоєння світових можливостей. Наразі ми не можемо знецінити роль таких важливих науково-технічних напрямків.

Література:

1. Карпенко В., Гіпотетичне майбутнє універсального штучного інтелекту. Філософія науки: традиції на інновації. 2011. №1 (3). С. 57-64.

2. Козлова О.В. Переваги експертних систем за традиційними системами штучного інтелекту. Системи озброєння і військова техніка. 2011. № 1 (25). С. 104–106.

3. Максим Баковецький, Роман Бараненко: Штучний інтелект і право, URL: https://www.businesslaw.org.ua/shtuchnyi-intelect-i-pravo-t/ (дата звернення: 26.04.21)

4. Бежевець А. М. Правовий статус роботів: проблеми та перспективи визанчення, URL: http://ippi.org.ua/sites/default/files/9_11.pdf (дата звернення: 26.04.21)

5. Каткова т. Г., Штучний інтелект в Україні: правові аспекти, URL: http://pravoisuspilstvo.Org.Ua/archive/2020/6_2020/10.Pdf (дата звернення : 26.04.21)

Післямова

Актуальність проекту «Європейська інтеграція: законодавство та Інтернет речей» у межах напряму Жан Моне «Модуль» програми «Erasmus+» №620017-EPP-1-2020-1-UA-EPPJMO-MODULE для України пов’язана з процесами європейської інтеграції у сфері цифрової трансформації, здебільшого, щодо процесу впровадження сучасних технологій Інтернету речей (IoT).

Йдеться про дослідження ролі ЄС у глобалізованому світі, зокрема, законодавства ЄС, яке стосується сфери інформаційних цифрових технологій в епоху розвитку досягнень четвертої технологічної революції.

Для реалізації цієї мети ми запропонували запровадити нову дисципліну - “Євроінтеграція: законодавство та Інтернет речей”.

Вона призначена для залучення широкого кола студентів, науковців, представників зацікавлених державних органів і громадських та неурядових організацій, практикуючих юристів, ІТ-спеціалістів.

Залучені учасники проекту можуть набути та вдосконалити свої професійні навички з:

1) правових питань впровадження IoT;

2) законодавства ЄС у галузі інформаційних технологій;

3) порівняльно-правового аналізу національного законодавства та законодавства ЄС у сфері IoT.

Це передбачає вивчення змісту, складу, особливостей, системних ризиків та бар’єрів використання IoT, а також роз’яснення політики ЄС щодо його розвитку.

Центральними темами курсу є юридичні питання забезпечення кібербезпеки, пов’язаної з IoT, в контексті захисту критичної інформаційної інфраструктури персональних даних та ідентифікації суб’єктів та об’єктів, що стосуються технологій IoT, використання роботів та штучного інтелекту, технологій хмарних обчислень та блокчейну.

Проект базується на інноваційних формах навчання. Це сприяє набуттю навичок самостійного пошуку, виявлення та вирішення юридичних проблем, пов’язаних із використанням IoT.

У цьому проекті також впроваджений інноваційний мультидисциплінарний підхід. Це дозволяє поєднувати знання з технічних та правових аспектів IoT. Це стає можливим завдяки унікальному поєднанню професіоналів з політехнічних та юридичних дисциплін Національного технічного університету України «Київський політехнічний інститут Ігоря Сікорського».

Наукове видання

ЗБІРНИК МАТЕРІАЛІВ
ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ІНТЕРНЕТ РЕЧЕЙ: ТЕОРЕТИКО-ПРАВОВІ ТА ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

29 квітня 2021 року, м. Київ