НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ТОКАРЕВА ВІРА ОЛЕКСАНДРІВНА

УДК 347.15/17:004.738.5

ДИСЕРАТАЦІЯ

ПРАВОСУБ'ЄКТНІСТЬ ФІЗИЧНОЇ ОСОБИ У ВІДНОСИНАХ У МЕРЕЖІ «ІНТЕРНЕТ»

Спеціальність 12.00.03 – цивільне право і цивільний процес; сімейне право; міжнародне приватне право

Подається на здобуття наукового ступеня доктора юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело_____ В.О. Токарева

Науковий консультант:
Харитонова Олена Іванівна,
доктор юридичних наук, професор
член-кореспондент НАПрН України,

Одеса – 2025

АНОТАЦІЯ

Токарева В.О. **Правосуб'єктність фізичної особи у відносинах у мережі «Інтернет».** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.03 – цивільне право і цивільний процес; сімейне право; міжнародне приватне право. – Національний університет «Одеська юридична академія», Одеса, 2025.

Дисертація є першим у вітчизняній науці цивільного права комплексним дослідженням теоретичних та практичних проблем правосуб'єктності фізичної особи у відносинах у мережі «Інтернет».

У роботі досліджені особливості формування концепції правосуб'єктності фізичної особи, виникнення, припинення та зміст правоздатності та дієздатності фізичної особи з урахуванням сучасного етапу розвитку відносин у мережі «Інтернет».

Запропоновано концепцію цифрової ідентичності фізичної особи у відносинах у мережі «Інтернет. Цифрова ідентичність у вузькому значенні – цифровий образ суб'єкту цивільних відносин (джерело персональних даних особи, акаунту (обліковий запис), який ідентифікує його у відповідних системах). У широкому значенні цифрова ідентичність розуміється як система усіх даних про суб'єкта цивільних правовідносин, без прив'язки до конкретного акаунта, в тому числі всі дані, які особа залишає у результаті активної та пасивної діяльності, за винятком даних, які не дозволяють ідентифікувати особу. Елементами цифрової ідентичності в широкому значенні є: акаунти, персональні дані, цифрові сліди, результати діяльності фізичної особи у вигляді публікацій, дописів, світлин та інших даних, за винятком анонімізованих персональних даних або псевдоанімізованих даних, обробка яких відбувається способом, який не дозволяє їх віднести до конкретної фізичної особи.

Аналіз підходів до цифрової ідентичності фізичної особи у відносинах у мережі «Інтернет» дозволив дійти висновку, що розмежування цифрової

ідентичності у вузькому та широкому значеннях проявляться у спадкових відносинах та доступі до цифрової спадщини після смерті фізичної особи.

Запропоновано розуміння права на цифрову ідентичність як особистого немайнового права, що належить кожній фізичній особі, обумовленого розвитком технологій, комплексного за своєю структурою та включаючого: право на визнання цифрової ідентичності, право перешкоджати будь-якому спотворенню та посяганню на цифрову ідентичність, яке здатне завдати шкоди фізичній особі.

Цифрова репутація як особисте немайнове благо в умовах розвитку соціальних мереж, шерингових платформ виходить за межі лише суспільної оцінки ділових, професійних якостей та здібностей фізичної особи, пов'язується з якостями та оцінками особи які персоніфікують її не лише поміж фахівців у галузі, а й решти користувачів цифрового середовища, безпосередньо впливає на можливість участі у комунікації, договірних відносинах, отриманні прибутку як в мережі «Інтернет», так і у фізичному світі.

Аналіз світових підходів до правового регулювання відносин в мережі Інтернет дозволив обґрунтувати, що момент виникнення правоздатності фізичної особи у відносинах у мережі Інтернет залежить від підходу держав до правового регулювання Інтернету. Здійснення прав в мережі «Інтернет» може істотно варіюватися залежно від механізмів правового регулювання прав та обов'язків користувачів та обраного державою підходу: ліберального – властивого західному підходу (ЄС, США) або авторитарного – властивого закритому, східному підходу регулювання Інтернету (КНР).

Внаслідок смерті фізичної особи відбувається трансформація цифрової ідентичності, перехід прав на цифрове майно та отримання спадкоємцями доступу до акаунтів особи в Інтернеті. Встановлено, що видалення акаунту та персональної інформації користувача, а з тим здійснення фізичною особою своєї правоздатності та дієздатності у мережі, може бути добровільним (за волевиявленням фізичної особи) і примусовим, застосовуватися в якості санкції за вчинення правопорушення за рішенням суду або порушення умов

користувацької угоди за рішенням Інтернет-сервісу. Користувач має право залишити розпорядження на цифровій платформі на випадок смерті, відносно долі цифрових речей, призначити осіб, яким має бути наданий доступ або розпорядитися про видалення акаунту.

Запропоновано поняття цифрової смерті як правової категорії, під якою розуміється видалення акаунту за життя людини або трансформація акаунту у цифровий меморіал у разі смерті особи. Категорія цифрової смерті може не співпадати з категорією смерті фізичної особи. Цифрова смерть може бути добровільною (мати підставою рішення фізичної особи) або ґрунтуватися на рішенні правонаступників (адміністраторів сторінки або платформи) у разі смерті фізичної особи. У зв'язку із розвитком електронного урядування та можливістю згенерувати акаунт фізичної особи в державних інформаційних системах, використання добровільного видалення акаунту користувачем може застосовуватися виключно у приватних інформаційних системах. Трансформації існуючого цифрового акаунту в меморіал після смерті користувача, не забезпечує спадкоємцям отримання доступу до цифрових активів, листування та контенту.

З огляду на обмеження розкриття функціонування коду алгоритму як об'єкту права інтелектуальної власності, запропоновано передбачити у законодавстві право суб'єктів даних на отримання інформації про логіку прийнятого індивідуального рішення (аналізу вхідних даних, статистичного пояснення, перевірки коду, визначення чутливих окремих даних та змінних, які зумовили результат) та кореспондуючий обов'язок контролера у разі прийняття рішення із застосуванням алгоритму надати інформацію суб'єкту даних про логіку індивідуального рішення, що лежить в основі обробки.

Запропоновано до системи цифрових прав включити право бути обізнаним про використання автоматизованих систем у прийнятті юридично значущих рішень та надати право суб'єктам даних оскаржувати юридично значущі рішення, які прийняті за участю автоматизованих систем.

З урахуванням розглянутих упереджень, що суб'єкти прийняття юридично значущих рішень схильні надмірно покладатися на рішення автоматизованих систем, ігноруючи власні судження, доведено, що остаточне рішення повинно ухвалюватися людиною. У таких сферах, як фінанси та судочинство попереднє рішення автоматизованої системи може призводити до настання несприятливих наслідків, суттєво обмежувати у здійсненні прав, затаврувати в суспільстві, внаслідок того, що суб'єкт прийняття юридично значущого рішення надає йому першочергового значення у своїй процедурі ухвалення рішення.

Запропоновано розрізняти види упереджень, які впливають на прийняття юридично значущих рішень із використанням автоматизованих систем: 1) структурні упередження, які виникають внаслідок програмування системи; 2) упередження в даних унаслідок функціонування системи, яка виводить певне значення у рівень еталону (нерепрезентативні дані); 3) алгоритмічні упередження, обумовлені тим, що суб'єкт надмірно покладається на рішення, прийняті алгоритмом, нехтуючи критичне мислення.

Проведений аналіз підходів до питання розкриття суб'єкту логіки прийнятих рішень алгоритмом, дозволив довести, що право на роз'яснення та обґрунтування прийняття конкретного автоматизованого юридично значущого рішення не забезпечено гарантіями, передбаченими ст. 22, та обов'язками контролерів надати доступ до даних згідно із ст. 13, 14 Регламенту ЄС 2016/679.

З урахуванням аналізу законодавства ЄС, доведено, що внаслідок цифрового профілювання створюються нові дані, які не є ідентичними тим, що були надані суб'єктом даних, а метод профілювання створює значні ризики для прав та свобод людини, коли людина може потрапляти в певні категорії, не знаючи про це. Профілювання може призводити до обмеження доступу до певних товарів та послуг, створювати дискримінацію та підвищувати ризики втручання у приватне життя.

З метою недопущення зловживання генетичними технологіями та дотримання прав людини, запропоновано доповнити: ст. 99 Закону України «Про страхування» положенням про заборону оцінки ризику на основі прогностичного

генетичного тестування, заборону страховиків вимагати проходження генетичного тестування та запитувати у застрахованих осіб або родичів надання результатів такого тестування; ст. 2-1 Кодексу законів про працю України положенням про заборону вимагати від працівників проходження генетичного тестування, подання його результатів, іншої інформації щодо генетичних особливостей працівника (його родичів) та будь-яку дискримінацію за генетичними ознаками.

Вдосконалено визначення біометричних даних в частині визнання персональних даних біометричними даними через застосування спеціальної технічної обробки фізичних, фізіологічних або поведінкових характеристик особи, з метою однозначної ідентифікації фізичної особи. Аргументовано розуміння цифрових прав як прав людини нового покоління та включення до їх числа, поряд із загальновизнаними правами людини, які здійснюються в мережі «Інтернет», права, обумовлені функціонуванням технологій (право на доступ до даних, видалення даних, виправлення та уточнення даних, на перенесення даних, обмеження обробки даних, заперечення проти обробки та проти прийняття значущого рішення на підставі автоматизованої обробки персональних даних та інші), та здійснення яких може забезпечуватись, разом із правовими засобами, програмним кодом. Вдосконалено розуміння права доступу до Інтернету як похідного від права на інформацію (здійснення права доступу до інфраструктури мережі Інтернету та до контенту), що вимагає від держав виконання позитивних (забезпечення підключення до мережі, якщо в місцевості відсутня необхідна інфраструктура) та негативних гарантій (невтручання у приватне життя, недопустимість масового обмеження доступу та блокування до ресурсів, недопущення переслідування користувачів на підставі політичних переконань та поглядів у мережі «Інтернет»).

Вдосконалено визначення права на інформаційну приватність, як особистого немайнового права особи контролювати обсяг та зміст інформації, пов’язаної зі збором та обробкою персональних даних, вимагати від контролерів виконання їх обов’язків щодо здійснення суб’єктом його прав: на доступ,

уточнення, перенесення, обмеження обробки, видалення персональних даних; заперечення проти обробки та обмеження обробки персональних даних із застосуванням автоматизованих систем; вимагати захисту порушених прав.

Аргументовано, що персональні дані визнаються біометричними даними в результаті застосування обробки фізичних, фізіологічних або поведінкових характеристик фізичної особи, з метою її однозначної ідентифікації.

З урахуванням судової практики та законодавства ЄС встановлено, що здійснення права суб'єкта даних на доступ до персональних даних може бути необхідною умовою здійснення права на виправлення даних, заперечення проти обробки, звернення до суду та третіх осіб для отримання компенсації. Здійснення права на доступ до даних має винятки, обумовлені неможливістю конкретної ідентифікації одержувачів, яким розкривались дані. Контролер має надати суб'єктам даних інформацію про одержувачів у разі несанкціонованого розголошення даних (витоку), за винятком неможливості їх ідентифікувати або у разі явно необґрунтованого або надмірного запиту суб'єкта даних, надати категорії відповідних отримувачів, не розкриваючи конкретних фактичних осіб.

З урахуваннями обов'язку контролерів підтримувати актуальні персональні дані, зростає значущість здійснення права суб'єкта на уточнення та надання додаткових даних. Обґрунтовано, що фізична особа може здійснити право на уточнення, доповнення та виправлення неповної інформації у первинних даних та результатах профілювання. Контролер має право відхилити надані суб'єктом уточнюючі персональні дані лише у випадку, якщо вони не відповідають меті його обробки.

Законодавство та судова практика ЄС передбачає обмеження здійснення права бути забутим, врівноважуючи інтереси контролерів даних та суб'єктів даних. Доведено, що право на забуття не застосовується, коли обробка персональних даних необхідна для: здійснення права на свободу вираження думки та свободу інформації; виконання завдань в інтересах суспільства або офіційних повноважень, покладених на контролера у галузі охорони здоров'я; архівування у суспільних інтересах, наукових та історичних дослідженнях,

статистичних та інших подібних цілей; здійснення судочинства. Здійснення права на забуття може полягати у видаленні посилання на публікацію у пошуковому запиті. Право на забуття не застосовується по відношенню до реєстраційних даних компаній, у разі виникнення колізії між правом на недоторканність приватного життя та забезпеченням прозорості ділових відносин.

Аргументовано необхідність встановлення стандартів функціонування систем ШІ та їх дотримання компаніями. Обґрунтовано необхідність інформування суб'єктів про використання автоматизованих систем у товарах, послугах та про право бути поінформованими про взаємодію саме з агентом ШІ, а не людиною. Інформування суб'єктів про використання автоматизованих систем може здійснюватися шляхом маркування товарів, робіт, публікацій (у разі внесення змін в новини, фото та відео) для запобігання введення суб'єктів в оману.

Аналіз правозастосовчої практики та доктрини щодо застосування автоматизованих систем та віддаленої біометричної ідентифікації яке поряд із позитивним впливом несе високі ризики для суб'єктів даних дозволило запропонувати у законодавстві положення про: 1) заборону використання технології віддаленої біометричної ідентифікації «в режимі реального часу»; 2) заборону невибіркової ідентифікації та прихованого відеоспостереження; 3) заборону використання систем соціального рейтингу (оцінки); 4) заборону використання технологій впливу на підсвідомість для маніпулювання, підбурювання до певної поведінки та прийняття рішень; 5) заборону проведення невибіркового або нецільового розпізнавання обличчя шляхом розширення баз даних за рахунок зображень облич із мережі «Інтернет», приватних баз даних та створення об'єднаних баз.

Ключові слова: правосуб'єктність фізичної особи, цифрова ідентичність, блокчейн, цифрові права, права людини, персональні дані, цифрова репутація, штучний інтелект, біометрична ідентифікація, програмний код.

ABSTRACT

Tokareva V.O. **The Legal capacity of a natural person in relations on the «Internet».** – Qualifying scientific work on the rights of the manuscript.

Dissertation for obtaining the degree of Doctor of Law in the specialty 12.00.03 – Civil Law and Civil Process; Family Law; Private International Law. – National University «Odesa Law Academy», Odesa, 2025.

The dissertation is the first comprehensive study of theoretical and practical issues of the legal capacity of a natural person in relations on the Internet in the national civil law doctrine.

The dissertation focuses on the unique aspects of the formation of the concept of legal capacity of a natural person, its emergence and termination, and the content of legal capacity of an individual at the current stage of society in relationships on the Internet.

The concept of digital identity of a natural person on the Internet is proposed. Digital identity in the narrow sense – a digital image of the subject of civil relations (the source of personal data and the account that identifies him in the relevant systems). In a broad sense, digital identity is understood as a system of all data related to the subject of civil relations, without reference to particular account, including all data of a natural person that generated through both active and passive activities, data that does not identify a natural person are excepted.

Elements of digital identity in a broad sense include accounts, personal data, digital traces, the outcomes of an individual's actions, such as publications, posts, photos and other data, with the exception of anonymized or pseudonymised data, the processing of which takes place in a way that does not allow them to be attributed to a specific person.

Based on the analysis of approaches to the digital identity of a natural person on the Internet, it can be concluded that the distinction between digital identity in a narrow and broad sense will be apparent in hereditary legal relationships and access to digital heritage after an individual's death.

According to the proposal, the right to digital identity is a personal non-property right, determined by technological advancement and belongs to each natural person.

The right to digital identity is intricately structured and encompasses the right to recognize digital identity, as well as the right to prevent any distortion or encroachment on digital identity that could be harmful to a natural person.

In the context of the development of social networks and sharing platforms, digital reputation is considered personal non-property rights that encompass both social assessment of an individual and business, as well as professional qualities and abilities. The ability to participate in communication, establish contracts and make profit both on the Internet and in the real world is directly affected by digital reputation, which is connected to the qualities and assessments that define a person among specialists and other users.

The legal capacity of an individual on the Internet depends on the approach of the regulation of legal relations of the Internet, as revealed by the analysis of global approaches to regulation of legal relations on the Internet. The state's approach and legal mechanisms that govern users' rights and obligations can greatly affect how they can exercise their rights on the Internet. There are two types of Internet regulation: liberal, which is a prevalent form in Western countries (EU, USA), and authoritarian, which is a prevalent form in Eastern countries (PRC).

The death of an individual results in their digital identity being transformed, their digital property being transferred, and their heirs being granted access to accounts on the Internet. The deletion of a user's account and personal information can be done either at their own will or by force. Forced deletion of an account can be used as a punishment for committing an offense or breaching the terms of the user agreement by the Internet service. In case of death, the user has the option to leave a will on the digital platform regarding the fate of digital things, appointing those who should be granted access, or order to deleting the account in case of death.

The legal concept of digital death is proposed as a legal category that encompasses the deletion of an account during a person's lifetime or the transformation of an account into a digital memorial on case of his death.

The category of digital death may not correspond to the category of human death. Digital death can be voluntary (based on an individual's decision) or based on the decision of legal successors (page or platform administrators) in the case of an individual's death. Due to the development of e-government and the ability to generate an individual's account in state information systems, voluntary deletion of accounts by the user can be used exclusively in private information systems. Transforming a memorial for an existing digital account after the user's death does not provide heirs with access to digital assets, correspondence and content.

Given the limitations on disclosing the functioning of algorithm codes as objects of intellectual property rights, it is suggested that the legislation should permit data subjects to have access to the logic of automated individual decision-making or righty to explanation (that is identifying the sensitive data and that led to the result can be achieved by analyzing input data, statistical explanation, providing statistical explanations and verifying codes) and the corresponding the controller's duty is to explain the data subject about the logic behind of the individual's decision.

Due to the biases that legal decision-making subjects frequently exhibit, which involve relying on automated systems and ignoring their own judgments, the final automated decision must be made by a person. In finance and litigation, a preliminary decision made by an automated system may have legal effects concerning the data subject, significantly limit their rights, and brand them in society as a result of the fact that the subject of a legally significant decision places it at the forefront of their decision-making process.

It is proposed to include in the digital rights system the right to be aware of the use of automated systems in decision that make significant impact on data subject and right to challenge decisions makes with the assistance of automated decision-making systems.

Various biases that affect the adoption of automated decision-making systems that make significant impact on data subject are proposed to be differentiated: 1) structural biases that arise as a result of system programming; 2) biases in data that arise due to the functioning of the system, which brings a certain value to the level of

the standard (unrepresentative data); 3) algorithmic biases that arise as a result of the subject excessively relying on algorithm decisions, neglecting critical thinking.

By analyzing approaches to the issue of disclosing logic of decisions made by the algorithms to the data subject it was possible to prove that the right to explanation regarding the adoption of a specific automated decision-making systems is not ensured by the guarantees provided in Art. 22 and the duties of controllers to provide access to data in accordance with Art. 13, 14 of EU Regulation 2016/679.

Taking into account the analysis of EU legislation, it is proven that as a result of digital profiling, new data created that are not identical to data provided by the data subject. The profiling method creates significant risks for human rights and freedoms when a natural person is profiled without knowing about it. Profiling can lead to limited access to certain goods and services, create discrimination and increase the risks of interference in private life.

To uphold human rights and prevent the abuse of genetic technologies the following rules are proposed to be included in the legislation: article 99 of the Law of Ukraine «On Insurance» with a provision prohibiting risk assessment based on prognostic genetic testing, prohibiting insurers from asking genetic testing and asking insured (his relatives) to give the results of testing; article 2-1 of the Labor Code of Ukraine with a provision prohibiting employees from undergoing genetic testing, submitting its results, other data regarding the genetic characteristics of the employee (his relatives) and any discrimination based on genetic characteristics.

The definition of biometric data has been enhanced to acknowledge that ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, with the aim of unambiguous identification of a natural person. The understanding of digital rights as human rights of a new generation, along with generally recognized human rights exercised on the Internet, determined by the functioning of technologies (the right to access data, to delete data, rectify data, to transfer data, restrictions on data processing, objections to processing and to making a significant decision on the basis of automated processing of personal data, etc.), and the implementation of which can

be ensured are argued together with legal means, software code. The understanding of the right to access the Internet as a derivative from the right to information (exercising the right to access the infrastructure of the Internet and content) has been improved, which requires states to fulfil positive (ensuring connection to the network if the necessary infrastructure is missing in the area) and negative guarantees (non-interference in private life, inadmissibility of mass restriction of access and blocking of resources, prevention of persecution of users on the basis of political beliefs and views on the Internet).

The definition of the right to information privacy has been improved, as a personal non-property right to control the information related to the collection and processing of personal data, to require controllers to fulfil their obligations regarding the subject's exercise of his rights: to access, clarify, transfer, limit the processing, delete personal data; object to the processing of personal data using automated systems; request protection of violated rights.

It is argued that personal data is recognized as biometric data through the use of special technical processing of physical, physiological or behavioural characteristics of a natural person, for the purpose of unambiguous identification of a natural person.

The right to access personal data is considered a necessary condition for exercising the right to rectify inaccurate data, object to processing, go to court, and receive compensation from third parties, according to judicial practice and EU law. The right to access data has exceptions due to the impossibility of specific identification of the recipients to whom the data was disclosed. The controller shall provide data subjects with information about the recipients in the case of unauthorised disclosure of the data, except when it is impossible to identify them or when the data subject makes a manifestly unreasonable or excessive request, providing categories of relevant recipients without disclosing the actual persons.

In terms of the information society, the obligation of controllers to maintain personal data up-to-date, the importance of exercising the subject's right to rectify and provide additional data is on the rise. Individuals have been determined to have the right to supplement and rectify inaccurate primary data and profiling results. The

controller has the right to reject the rectifying personal data provided by the subject only if it does not correspond to the purpose of its processing.

EU legislation and doctrine stipulate that the right to be forgotten (right to erasure) is limited, balancing the interests of data controllers and data subjects. It has been proven that the right to be forgotten does not pertain when the processing of personal data is necessary for: the exercise of the right to freedom of expression and information; the performance of tasks in the public interest or exercising official powers given to the controller in health care; archiving in the public interest, scientific and historical research, statistical and other similar purposes; the implementation of judicial proceedings. Exercising the right to be forgotten may consist of deleting the link to the publication in the search query. The right to be forgotten is not applicable to company registration data, in case of a conflict between the right to privacy and transparency of business relations.

The need to establish standards for the functioning of AI systems and their compliance by companies is argued. The need to inform subjects about the use of automated systems in goods and services is backed up. The right to be informed about interactions with an AI agent, not a person, is substantiated. Informing subjects about the use of automated systems can be done by marking goods, works, publications (in case of changes in news, photos and videos) to prevent subjects from being misled.

The analysis of law enforcement practice and doctrine has made it possible to assert that the use of automated systems and remote biometric identification, despite its positive impact, poses a significant risk for data subjects. In order to uphold human rights in the context of digitalization, it is suggested to include this provision in the legislation: 1) prohibition of the use of remote biometric identification technology «in real time»; 2) prohibition of indiscriminate identification and hidden video surveillance; 3) prohibition of the use of social scoring (evaluation) systems; 4) prohibition of the use of subliminal technologies to manipulate, incite certain behaviour and make decisions; 5) prohibition of conduct of indiscriminate or non-targeted facial recognition by expanding databases to include images of faces from the Internet, private databases and the establishment of pooled databases.

Key words: legal capacity of a natural person, digital identity, blockchain, digital rights, human rights, personal data, digital reputation, artificial intelligence, biometric identification, program code.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Наукові, праці в яких опубліковані основні наукові результати дисертації:

1. Токарева В.О. Наслідки порушення прав інтелектуальної власності китайськими товаровиробниками. *Часопис цивілістики.* 2016. № 20. С. 202-206. URL: http://clj.nuoua.od.ua/archive/20/43.pdf

2. Токарева В.О. Авторське право у цифрову добу. *Часопис цивілістики.* 2017. №26. С. 93-98. URL: http://clj.nuoua.od.ua/archive/26/22.pdf

3. Токарева В.О. Інтелектуальна власність КНР: на шляху інновацій. *Науковий Вісник МГУ.* 2018. № 32. С. 53-56. URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc32/14.pdf

4. Токарева В.О. Щодо питання творчості та штучного інтелекту. *Прикарпатський юридичний вісник.* 2018. № 1(22). С. 55-58. URL: http://pjv.nuoua.od.ua/v1_2018/15.pdf

5. Токарева В.О. Онлайн платформи: виклик авторському праву у цифрову добу. *Часопис цивілістики.* 2018. № 29. С. 107-111. URL: http://clj.nuoua.od.ua/archive/29/23.pdf

6. Токарева В.О. Обчислювальна творчість (щодо питання творчості штучного інтелекту). *Часопис цивілістики*. 2018. № 30. С. 38-43. URL: http://clj.nuoua.od.ua/archive/30/10.pdf

7. Токарева В.О. Щодо питання інформаційної природи авторського права. *Часопис цивілістики.* 2019. № 33. С. 61-66. URL: http://clj.nuoua.od.ua/archive/33/13.pdf

8. Токарева В.О. Умови охороноздатності об'єктів авторського права. *Приватне та публічне право.* 2019. № 3. 39-43. URL: http://www.pp-law.in.ua/archive/3_2019/11.pdf

9. Токарева В.О. Похідні твори у галузі сучасного мистецтва. *Науковий вісник публічного та приватного права.* 2019. № 6. С. 35-40. URL: http://nvppp.in.ua/vip/2019/6/7.pdf

10. Токарева В.О. Сумлінне використання та похідні твори у сучасному мистецтві. *Таврійський національний університет імені В.І. Вернадського.* 2020. Т. 31 (70). № 2. С. 121-125. URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_1/25.pdf

11. Токарева В.О. Щодо питання захисту прав інтелектуальної власності. *Часопис Цивілістики.* 2020. №. 36. 51-56. URL: http://clj.nuoua.od.ua/archive/36/11.pdf

12. Токарева В.О. Формування категорії «віртуальна ідентичність» у мережі Інтернет. *Часопис Цивілістики*. 2022. № 45. С. 63-67. URL: http://chascyvil.onua.edu.ua/index.php/chc/article/view/468/511

13. Токарева В.О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 3. С. 47-52. URL: http://apnl.dnu.in.ua/3_2022/8.pdf

14. Токарева В.О. Окремі питання реалізації права на видалення. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 4. С. 43-47. URL: http://apnl.dnu.in.ua/4_2022/8.pdf

15. Токарева В.О. Щодо визначення персональних даних в умовах Євроінтеграційних процесів. *Південноукраїнський правничий часопис.* 2022. № 4. Том 3. С. 169-174 URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_3/28.pdf

16. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Публічне та приватне право.* 2022. № 4. С. 35-40. URL: http://pp-law.in.ua/archive/4_2022/6.pdf

17. Токарева В.О. До питання прийняття рішень із застосування алгоритмів**.** *Публічне та приватне право.* 2023. № 1. С. 30-35. URL: http://pp-law.in.ua/archive/1_2023/5.pdf

18. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики.* 2023. № 49. С. 32-37. URL: http://clj.nuoua.od.ua/archive/49/5.pdf

19. Токарева В.О. Правове регулювання застосування систем віддаленої біометричної ідентифікації в ЄС. *Публічне та приватне право.* 2023. № 2. С. 3-8. URL: http://pp-law.in.ua/archive/2_2023/1.pdf

20. Токарева В. Реалізація сімейної правоздатності фізичної особи за допомогою мережі Інтернет. *Юридичний бюлетень.* № 29. 2023. С. 134-141. URL: http://www.lawbulletin.oduvs.od.ua/archive/2023/29/14.pdf

21. Токарева В.О. Порушення прав на торговельні марки в мережі Інтернет. Юридичний науковий електронний журнал. 2023. №10. С.141-144. URL: http://www.lsej.org.ua/10_2023/32.pdf

22. Токарева В.О. Окремі питання управління майном фізичної особи**.** *Юридичний науковий електронний журнал.* 2024. № 4. С.129-131. URL: http://www.lsej.org.ua/8_2024/30.pdf

23. Токарева В.О. До питання права на зображення (голограму) фізичної особи після смерті в умовах поширення технологій ШІ. *Часопис цивілістики.* 2024. № 54. С. 43-48. URL: http://clj.nuoua.od.ua/archive/54/8.pdf

24. Токарева В.О., Личко В.С. Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С. 848 -851. URL: http://www.lsej.org.ua/4_2024/209.pdf

25. Токарева В.О., Личко В.С. Спадкування об’єктів в мережі Інтернет: досвід західних держав. *Часопис цивілістики.* 2024. № 53. С. 41-46. URL: http://clj.nuoua.od.ua/archive/53/9.pdf

26. Давидов І.В., Токарева В.О. Захист права на повагу до честі та гідності, ділової репутації, публічних осіб. *Держава та регіони. Серія Право.* 2022. № 1 (75). С. 131-135. URL: http://www.law.stateandregions.zp.ua/archive/1_2022/22.pdf

27. Давидова І.В. Токарева В.О. Цифрова нерівність. Цифрова нерівність і право на доступ до Інтернету. *Юридичний вісник***.** 2024. № 6. С. 68-75. URL: http://yurvisnyk.in.ua/v6_2024/10.pdf

Наукові праці, статті у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection та Scopus:

28. Nekit K., Tokareva V., Zubar V. Artificial intelligence as a potential subject of property and intellectual property relations. *Ius Humani. Law Journal*. 2020. № 9 (1). P. 231-250. URL: https://doi.org/https://doi.org/10.31207/ih.v9i1.227

29. Tokareva V. Davydova I., Adamova E. Legal problems of the use of orphan works in digital age. *Juridical Tribune.* 2021. № 11. P. 453-471. URL: http://www.tribunajuridica.eu/arhiva/An11v3/3.%20Tokareva%20Davydova%20Adamova.pdf

30. Davydova I., Zhurylo S., Tomina V., Fuchedzhi V., Tokareva V. Legal aspects of the regulation of social relations with the participation of Artificial Intelligence. *Revista De La Universidad Del Zulia*. 2022. № 13(38). P. 487-500. DOI: http://dx.doi.org/10.46925//rdluz.38.28

31. Davydova I., Nahnybida V., Adamova O., Zhurylo S., Tokareva V. Blockchain and civil proceedings: points of convergence. *DIXI*. 2022 (2023). № 25(1). P. 1–20. URL: https://revistas.ucc.edu.co/index.php/di/article/view/4637

32. Davydova I., Bernaz-Lukavetska O., Tokareva V., Andriienko I., Tserkovna O. Freedom of contract in the digital age and its implementation in modern technologies: theory and practice. *International Journal of Computer Science and Network Security*. 2022. № 12 (21). P. 544-548. URL: http:// paper.ijcsns.org/07_book/202112/20211275.pdf

Наукові статті у зарубіжних періодичних виданнях юридичного напряму:

33. Токарева В.О. Проблемні питання творчості в умовах цифрової доби. *European political and law discourse.* 2019. № 2. С. 123-128. URL: https://eppd13.cz/wp-content/uploads/2019/2019-6-2/eppd_2019_6_2.pdf

34. Токарева В.О. Окремі аспекти сирітських творів в умовах інтеграційних процесів. *Jurnaluljuridic.* 2019. №3. С. 97-101. URL: http://www.jurnaluljuridic.in.ua/archive/2019/3/part_1/22.pdf

35. Токарева В.О. Обчислювальна (Алгоритмічна) творчість: постановка проблеми. *Visegrad Jurnal on Human Rights.* 2019. № 2. (V.2) С. 150-155. URL: https://journal-vjhr.sk/wp-content/uploads/2020/12/Vyshegrad-2_2019_Tom-2.pdf

36. Токарева В.О. Окремі питання легалізації сирітських творів. *Recht der Osteuropäischen Staaten (ReOS).* 2019. №1. С. 197-201. URL: https://www.uni-goettingen.de/de/document/download/ca207b2c626da0c3a651dab3e413069e.pdf/ReOS%2001%20aus%202019.pdf

Наукові праці які засвідчують апробацію матеріалів дисертації:

37. Токарева В.О. Дискусійні питання алгоритмічної творчості. *Розвиток державності та права в Україні реалії та перспективи*: матеріали міжнародної науково-практичної конференції. (м. Львів, 20-21 вересня 2019 р.). Львів: Західноукраїнська організація «Центр правничих ініціатив», 2019. С. 42-46.

38. Токарева В.О. Дотримання GDPR в умовах COVID-19. *Інформаційні технології в умовах оновлення цивільного законодавства*: матеріали. Всеукр. кругл. столу (м. Одеса, 13 черв. 2020 р.) За заг. ред. О. І. Харитонової, Є. О. Харитонова. Одеса: Фенікс, 2020. С. 60-62.

39. Токарева В.О. Щодо окремих питань творчості штучного інтелекту. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-ти річчя проголошення незалежності України та 25-ти річчя прийняття Конституції України):* матеріали Міжнародної науково-практичної конференції (21 травня 2021 р.). Одеса: Причорноморська фундація права. С. 352-356.

40. Токарева В.О. Проблемні аспекти творчості в епоху цифрових трансформацій. *Взаємодія громадянського суспільства, особи і держави:* вектор удосконалення: матеріали Міжнародної науково-практичної конференції. (м. Київ, 22 червня 2021р.). Київ: Київський регіональний центр НАПрН, 2021. С. 179-182.

41. Токарева В.О. Проблеми легалізації сирітських творів в умовах інформаційного суспільства. *Проблеми та стан дотримання і захисту прав людини в Україні*: Матеріали міжнародної науково-практичної конференції (м. Львів, 20–21 серпня 2021 р.). Львів: Західноукраїнська організація «Центр правничих ініціатив», С. 31-34.

42. Токарева В.О. Окремі питання реалізації права на творчість особами засудженими до позбавлення волі. *Юридична наука: виклики і сьогодення*: матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 11–12 червня 2021 р.). Одеса: ГО «Причорноморська фундація права», 2021. С. 49-52.

43. Токарева В.О. Еволюція концепту творчості та розвитку інновацій в КНР. *Сучасне правотворення: питання теорії та практики* : Матеріали міжнародної науково-практичної конференції (м. Дніпро, 4–5 червня 2021 р.). Дніпро: ГО «Правовий світ», 2021. С. 51-54.

44. Токарева В.О. До питання результатів інтелектуальної діяльності та штучного інтелекту. *Особливості розвитку законодавства України у контексті євроінтеграційних процесів*: міжнародна науково-практична конференція (м. Харків, 4–5 червня 2021 р.). Харків: Східно-українська наукова юридична організація, 2021. С. 68-71.

45. Токарева В.О. Результати творчості сгенеровані штучним інтелектом. *Сучасний вимір держави і права*: матеріали міжнародної науково-практичної конференції (м. Львів, 18–19 червня 2021 р.). Львів: Західноукраїнська організація «Центр правничих ініціатив», 2021. С. 102-106.

46. Токарева В.О. Право на свободу вираження творчості. *Актуальні питання реформування правової системи України*: матеріали міжнародної науково-практичної конференції (м. Дніпро, 2–3 липня 2021 р.). Дніпро: ГО «Правовий світ», 2021. С. 17-20.

47. Токарева В.О. Окремі аспекти вираження творчості в умовах цифрових трансформацій. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI*

століття (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права): у 2 т.: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса: Видавничий дім «Гельветика», 2022. Т. 2. 2022 . С. 659-662.

48. Токарева В.О. Деякі питання щодо категорії «віртуальна ідентичність» у мережі Інтернет. *Integration of Education, Science and Business in Modern Environment: Summer Debates*: Proceedings of the 4th International Scientific and Practical Internet Conference (August 15-16, 2022.). Dnipro: FOP Marenichenko V.V. С. 67-69.

49. Токарева В.О. Деякі питання щодо категорії «віртуальна ідентичність» у мережі Інтернет. *Розвиток громадянського суспільства як необхідна складова європейської інтеграції України*: матеріали Всеукраїнської науково -практичної конференції (м. Київ, 06 жовтня 2022 р.). Львів-Торунь: Liha-Pres, 2022. С. 292-295.

50. Токарева В.О. Право на видалення та право на чистий цифровий лист. *Правове регулювання суспільних відносин: перспективні напрями на шляху до сталого розвитку*: матеріали Міжнародної науково-практичної конференції (м. Київ, 28-29 жовтня 2022 р.). Львів: Торунь: Liha-Pres, 2022. С. 46-50.

51. Токарева В.О. Щодо питання цифрової ідентичності в умовах війни. *Приватне право в умовах війни*: матеріали всеукр. наук. конф. (Одеса, 15 листоп. 2022 р.). за заг. ред.: д.ю.н., проф. Є. Харитонова, д.ю.н., проф. І. Давидової. Одеса: НУ «Одеська юридична академія. 2022. С. 111-116. URL: https://hdl.handle.net/11300/25131

52. Tokareva V. Digital identity as the element of concept of service-oriented state. *International Conference Challenges of Business Law in the Third Millennium* (Bucharest, November 25, 2022). Doctrina et Usu in Business Law. Contributions to the 12th. Bucharest: ADJURIS. P. 281-301.

53. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Становлення та розвиток правової держави: проблеми теорії та практики:* Матеріали XV міжнародної науково-практичної конференції, що присвячена

102-річчю Національного університету кораблебудування імені адмірала Макарова, м. Миколаїв. 28–29 грудня 2022 р. Львів-Торунь: Liha-Pres, 2022. С. 351-364.

54. Токарева В.О. Фізична особа в мережі Інтернет. *Актуальні проблеми протидії корупції в Україні в умовах воєнного стану*: матеріали Міжнародної науково-практичної конференції (м. Рівне, 14 березня 2023 року). Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука. Львів: Торунь: Liha-Pres, 2023. 176 с. С. 16-19.

55. Токарева В.О. До питання виникнення правосуб'єктності фізичної особи у мережі Інтернет. *І Міжнародна науково-практична конференція Таврійського національного університету до 160-ї річниці від дня народження В. І. Вернадського:* матеріали Міжнародної науково-практичної конференції, 16-17 березня 2023 р., м. Київ. Частина 1. Львів Торунь: Liha-Pres, 2023. С. 57-61.

56. Токарева В.О. Правове регулювання прийняття рішень із використанням алгоритмів. *Topical issues of modern jurisprudence*: International scientific conference proceedings (April 5–6, 2023. Częstochowa, the Republic of Poland). Riga, Latvia: «Baltija Publishing», 2023. С. 84-88.

57. Токарева В.О. До питання реалізації права відмовитися від ознайомлення із результатами медичних досліджень (право не знати). *Гармонізація законодавства України з правом Європейського Союзу: реалії та перспективи*: Всеукраїнська науково-практична конференція (м. Запоріжжя, 18 травня 2023 р.). Львів-Торунь: Liha-Pres, 2023. С. 169-173.

58. Токарева В.О. До питання прийняття юридично значущих рішень із застосування алгоритмів. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень*: у 2 т.: матеріали Міжнар. наук.- практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редак- цією С. В. Ківалова. Одеса: Юридика, 2023. – Т. 2. С. 534-537.

59. Токарева В.О. Правове регулювання транскордонної обробки персональних даних між ЄС та США. *Римське право і сучасність: актуальні*

проблеми оновлення цивільного законодавства: матер. Всеукр. наук. конф. (м. Одеса, 25 травня 2023 р.) [Електронне видання] / упоряд.: І. Давидова, М. Лєсняков ; за заг. ред. д.ю.н., проф. Є. О. Харитонова. Одеса, 2023. С. 80-85.

60. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень в США. *Проблеми цивільного права у постпандемічну добу*: матер. круг. столу (м. Одеса, 26 травня 2023 р.) [Електронне видання] / укл.: І.В. Давидова, О.В. Шамота; за ред.: Є.О. Харитонова, І.В. Давидової; Нац. ун-т «Одес. юрид. академія». Одеса, 2023. С. 60-64.

61. Токарева В.О. До питання персонанальних даних за законодавством ЄС. *Legal science, legislation and law enforcement: traditions and new European approaches*: International scientific conference proceedings (Wloclawek, May 29-30, 2023). Riga, Latvia: «Baltija Publishing», 2023. 124 pages. С. 39-43.

62. Токарева В.О. До питання дистанційної біометричної ідентифікації. Восьмі Таврійські юридичні наукові читання: матеріали міжнародної науково-практичної конференції (м. Київ, 16–17 червня 2023 р.). Львів –Торунь: Liha-Pres, 2023. С.62-66.

63. Токарева В.О. Окремі питання збору та обробки геномної інформації людини. *Договори в умовах миру та війни (до 90-річчя з дня народження В. Луця)*: матеріали Всеукр. наук. конф. [Електронне видання] / за заг. ред. Є. Харитонова, І. Давидової ; НУ «Одес. юрид. академія». Одеса: Фенікс, 2023. С. 52-57. URL: https://hdl.handle.net/11300/27420

64. Токарева В.О. До питання «persona» за римським правом. Цивілістичні проблеми спортивного права: матеріали Круглого столу, (Одеса, 28.10.2023 р.). [Електронне видання] / за заг. ред.: Є. Харитонова, І. Давидової, М. Ткалича; Нац. ун-т «Одес. юрид. академія». Одеса: Фенікс, 2023. С. 41-43. URL: https://hdl.handle.net/11300/27371

65. Токарева В.О. До питання репутації у мережі Інтернет. *Європейські орієнтири розвитку України*: науково-практичний вимір в умовах воєнних

викликів: матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. Одеса : Фенікс, 2024. С. 591-594.

66. Токарева В.О. До питання цифрової ідентичності та анонімізованих даних. *Римське право і сучасність: реалізація і захист речових прав в умовах воєнного стану*: матеріали Всеукр. наук. конф. (Одеса, 25 трав. 2024 р.) [Електронне видання] / за заг. ред.: Є. Харитонова, І. Давидової, В. Зубара; НУ «Одес. юрид. академія». Одеса: Фенікс, 2024. С. 11-114.

67. Токарева В.О. До питання цифрового громадянства. *Одеські грудневі цивілістичні читання: приватне право, як концепт в умовах війни, людський вимір*: матеріали Всеукр. наук. конф. (Одеса, 12 груд. 2024 р.) [Електронне видання] / за заг. ред.: д.ю.н., проф. Є. Харитонова, д.ю.н., проф. І. Давидової; НУ «Одес. юрид. академія». Одеса: Фенікс, 2025. С. 71-75. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/a2cd872f-d57a-4558-adaa-2cb9f2969520/content

Наукові праці, які додатково відображають наукові результати дисертації:

68. Токарева В.О. Зловживання цивільним правом та право на інформацію. Права приватної особи в умовах пандемії COVID-19: проблеми здійснення і захисту: монографія / Є.О. Харитонов, О.І. Харитонова, К.І. Бєляков; Є.О. Харитонова, О.І. Харитонової, К.Г. Некіт. Одеса: Гельветика, 2020. С. 194-204.

69. Токарева В.О. Обмеження майнових прав інтелектуальної власності у сфері охорони здоров'я. Приватні та публічні інтереси в умовах COVID-19: колізії та правові шляхи вирішення. колективна монографія; за ред. Харитонова Є.О., Харитонова О.І., Булеца С.Б. Одеса 2021. С. 279-293.

70. Токарева В.О. Розвиток цифрової ідентичності як елементу сервісної держави в умовах війни. Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: монографія [Електронне видання] / за ред.: Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт; упор.-укл. Ю.С. Маршук; НУ «Одеська юридична академія». Одеса: Фенікс, 2023. С 86-97.

71. Токарева В.О. Віртуальна ідентичність як проекція фізичної особи у мережі Інтернет. The European dimension of modern legal science: Scientific monograph. Riga, Latvia: Baltija Publishing, 2022. С. 406-418.

72. Токарева В.О. Анонімність в мережі Інтернет. Law in the postmodern epoch: general characteristics and manifestation particularities in separate law branches: Scientific monograph. Riga, Latvia: Baltija Publishing, 2023. С. 611-617.

73. Токарева В.О. Інформаційна приватність за законодавством ЄС: виклики та перспективи. Modern paradigm of public and private law amidst sustainable development: Scientific monograph. Vol. 2. Riga, Latvia: Baltija Publishing, 2023. С. 295-310.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ……..…4

ВСТУП…….5

1. ГЕНЕЗИС ТА ЮРИДИЧНА ПРИРОДА ФІЗИЧНОЇ ОСОБИ У МЕРЕЖІ «ІНТЕРНЕТ»……..25

1.1. Вибір напрямів дослідження…….……25

1.2. Мережа як чинник трансформації юридичної природи фізичної особи…….…. 42

2. ДОКТРИНАЛЬНІ ТА ПРАКТИЧНІ ПІДХОДИ ДО ФОРМУВАННЯ ЦИФРОВОЇ ІДЕНТИЧНОСТІ В МЕРЕЖІ «ІНТЕРНЕТ»……59

2.1. Концептуальні підходи до визначення права на цифрову ідентичність у мережі «Інтернет»……..…59

2.2. Формування концепції цифрової ідентичності фізичної особи в мережі «Інтернет»…….…..95

2.3. Ідентифікація фізичної особи у відносинах у мережі «Інтернет»…...125

2.4. Ідентифікуючі ознаки фізичної особи у відносинах у мережі «Інтернет»…….....148

3. ЦИВІЛЬНА ПРАВОЗДАТНІСТЬ ТА ДІЄЗДАТНІСТЬ ФІЗИЧНОЇ ОСОБИ У ВІДНОСИНАХ У МЕРЕЖІ «ІНТЕРНЕТ»: ЛЕГАЛЬНІ ПІДХОДИ І ДОКТРИНАЛЬНІ ТЛУМАЧЕННЯ……181

3.1. Виникнення і припинення правоздатності та дієздатності фізичної особи в мережі «Інтернет»……..181

3.2. Зміст цивільної правоздатності фізичної особи в мережі «Інтернет»…….……210

3.3. Особисті немайнові права у складі цивільної правоздатності фізичної особи в мережі «Інтернет»……..……232

3.3.1. Право на недоторканність приватного життя в мережі «Інтернет»…….....232

3.3.2. Право на доступ до мережі «Інтернет»……..263

3.3.3. Окремі цифрові права……..…….....…283

3.4. Основні положення про дієздатність фізичної особи у відносинах у мережі «Інтернет»…….. 351

ВИСНОВКИ…….……....370

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….391

ДОДАТКИ……..……...491

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ANT – акторно-мережева теорія;

BREXIT – Britain Exit;

GAFA – Google, Apple, Facebook, Amazon або **GAFAM** Google, Apple, Facebook, Amazon;

CNIL – (The *Commission nationale de l'informatique et des liberté)* Національна комісія Франції з інформаційних технологій та громадянських свобод;

ЗДПЛ – Загальна декларація прав людини;

ЄС – Європейський Союз;

ЄСПЛ – Європейський суд з прав людини;

ЄКПЛ – Європейська конвенція з прав людини;

КНР – Китайська Народна Республіка;

МПГПП – Міжнародний пакт про громадянські і політичні права;

Суд ЄС – Європейський Суд Справедливості;

IoT – (Internet of things) Інтернет речей;

MIT – Massachusetts Institute of Technology;

ПК України – Податковий кодекс України;

СК України – Сімейний кодекс України;

VR – (virtual reality) віртуальна реальність;

ШІ – штучний інтелект;

ЦК України – Цивільний кодекс України;

ЦПК України – Цивільний процесуальний кодекс України;

абз. – абзац;

п. – пункт;

ст. – стаття;

ч. – частина.

ВСТУП

Обґрунтування теми дослідження. Двадцять років тому до інтернету можна були увійти та вийти, проникнення інформаційно-комунікаційних технологій було низьким, віртуальна реальність порівнювалася з фізичною. Сучасне життя характеризується взаємозалежність між віртуальним та фізичним життям, де портативні технології, стирають межі між публічним та приватним, коли людина прагне продемонструвати своє життя в соціальних мережах.

В умовах розвитку інновацій, технологій IoT, віртуальної реальності, які забезпечують цілодобовий, безперервний доступ до інтернету, перебуваючи в офлайні, повідомлення поступають на екрани смартфонів, годинників нагадують про потребу негайного повернення в онлайн, межі фізичного світу та віртуального безповоротно втрачаються, а павутиння мереж вплітається у реальне буття людини. Комп'ютер перетворився в тоненький планшет, кишеньковий смартфон та окуляри, що свідчить про взаємопроникнення віртуального та реального світів, забезпечення постійного підключення до мережі.

Повноцінне використання новітніх технологій та участь у мережі є умовою здійснення прав людини, участі в соціальному та політичному житті. У мережі «Інтернет» людина представлена системою даних – цифровим акаунтом або цифровою ідентичністю. Поряд із цим зростає роль штучного інтелекту, так званої «чорної скриньки», яка збирає та аналізує дані суб'єктів у мережі, навчається та майже набуває здатності приймати окремі самостійні рішення. Наразі на підставі аналізу профайлу людини (набору персональних даних), «чорній скриньці» поступово делегують повноваження приймати юридично значущі рішення: щодо видачі кредиту, працевлаштування, у сфері судочинства тощо. Крім того, розвиток сучасних технологій, серед яких дистанційна біометрична ідентифікація, не лише за обличчям, а й манерою руху, людина може бути ідентифікована, дозволяючи створити диктатуру на зразок Дж. Орвелла та авторів інших антиутопій.

Поряд із зростанням обсягів збирання та автоматизованої обробки даних, порушенням правил транскордонної передачі персональних даних з ЄС до США, публічним викриттям та переслідуванням Е. Сноудена та Дж. Ассанджа, скандалів із маніпулюванням персональними даними під час політичних перегонів США та BREXIT, регулярних хакерських атак із витоком персональних даних, у суспільстві стали зростати побоювання втручання у приватне життя, стеження та прослуховування. Крім того, аналіз великих даних для розвитку машинного навчання ставить питання встановлення правових гарантій захисту прав особи на недоторканність приватного життя, прозорості застосування систем автоматизованого прийняття рішень та збереження контролю людини, недопущення випадків прийняття рішень виключно системами, без участі людини.

Поширення використання автоматизованих систем та технологій великих даних державними органами обумовлюється метою забезпечення національної безпеки та підвищенням рівня ефективності державних послуг, запобігання вчинення правопорушень тощо. У діяльності комерційних компаній (транспортних організацій, фінансових установ, маркетингових компаній тощо) – технології, використовується для гарантування безпеки, полегшення доступу до послуг, персоналізованої реклами та профілювання користувачів. За таких умов, особливого значення набуває дослідження та розробка положень щодо здійснення правосуб'єктності фізичної особи у відносинах у мережі «Інтернет».

Все викладене свідчить про недостатньо високий рівень розробленості в сучасній науці проблеми визначення поняття змісту та здійснення цивільної правосуб'єктності фізичної особи в мережі «Інтернет», яка несе істотне наукове та практичне значення, в результаті відсутності фундаментальних досліджень даної проблеми, здатних реалізувати комплексний підхід до розв'язання із врахуванням досвіду, накопиченого за історію становлення та розвитку категорії цивільна правосуб'єктність у вітчизняному та зарубіжному законодавстві.

Окремим аспектам правосуб'єктності та особливості здійснення прав та обов'язків фізичної особи в мережі «Інтернет» були присвячені низка

досліджень, серед яких необхідно назвати праці таких вчених як: Н.В. Баловсяк, Я.О. Берназюк, С.Б. Булеца, О.Б. Братасюк, В.М. Брижко, О.Б. Бутнік-Сіверський, Н.В. Верлос, В.О. Володавська, Н.В. Волкова, М.К. Галянтич, О.І. Гапченко, О.М. Головко, Н.Ю. Голубєва, О.А. Гончаренко, О.П. Горпинюк, О.С. Грабовська, П.Д. Гуйван, І.В. Давидова, В.М. Зубар, О.М. Калітенко, О.О. Кармаза, М.В. Карандась, О.О. Кулініч, Г.В. Лебедєва, В.О. Мацик, Н.С. Марценко, Р.А. Майданик**,** Л.Р. Майданик, Є.О. Мічурін, Д.О. Міський, М.В. Менджул, Н.Ф Ментух, І.В. Мукомела, К.Г. Некіт, П.А. Прохоров, О.Е. Радутний, І.Е. Ревуцька, Р.В. Романов, Д.А. Самодурова, О.М. Сафончик, В.А. Січевлюк, В.О. Серьогін, Р.О. Стефанчук, М.О. Стефанчук, В.А. Сокуренко, Т.О. Софіюк, Л.Л. Тарасенко, Н.О. Тищук, В.Г. Пилипчук, К. І. Пономаренко, Ю.С. Размєтаєва, М.Г. Хаустова, Є.О. Харитонов, О.І. Харитонова, Н.О. Хрякова, М.Р. Чалабієва, С.А. Чванкін, Р.Б. Шишка, Т.М. Ямненко та ін.

Особливості впливу мережі та інформаційно-комунікаційних технологій на здійснення правосуб'єктності фізичної особи можна знайти в роботах зарубіжних науковців та практиків, які використані в дисертаційному дослідженні: Дж. Балкін, Л.А. Байгрейв, А. Бернар, Ф. Боско, Н. Бостром, М.Т. Вагнер, С. Вахтер, Л. Вайн, Е. Вайценбек, А. Т. Віддісон, Ст. Веттіг, Дж. Гакутан, П. Герт, М. Гільдебрандт, Дж. Де Грегоріо, С. Дікін, К. Годард, Т. Грепель, Дж. Даніель, Дж. Б. Дюклерк, К. Духігг, К.Д. Ешлі, Х. Ейденмюллер, А. Зенос, Е. Зехенднер, Р. Кало, Б. Кастерс, Дж. Карйот, Р.А. Кларк, Т. Колдерс, С. Коколакіс, М. Косінскі, К. Крістенсен, Я. Коксвік, Л. Лессіг, І. Ллойд, К. Мартін, В. Маджид, Г. Мальгері, Р.Е. Менсел, В.Н. Мортеза, П. Норвиг, М. Овермарс, О. Полічіано, С. Ранчордас, Дж. Ракка, С. Рассел, К. Саліван, Н. Селвадурай, С.М. Солайман, Д. Дж. Солове, С. Смед, Д. Стіллвелл, Р. Стюарт, Г. Терпстра, М. Фазліоглу, Дж. Фаррар, Л. Флоріді, Н. Ф'юрі, С.Д. Хасслер, Б.А. Херршафт, Дж. Ван Гобокен, Є. Ціммерман, С. Чопра, Д. Чен, А. Шафер, П.М. Шварц, Е. Швайгофер та ін.

Утім, незважаючи на те, що проблемам правосуб'єктності фізичної особи були присвячені низка праць вітчизняних та зарубіжних науковців, на сьогодні все ще не вироблено єдиного підходу до розуміння поняття та сутності

правосуб'єктності фізичної особи, залишаються дискусійними питання стосовно змісту прав фізичної особи в мережі «Інтернет». Не вистачає досліджень, присвячених визначенню новітніх прав, обумовлених розвитком автоматизованих інформаційно-комунікаційних систем та їх впливу на переосмислення традиційних прав. У вітчизняній науці цивільного права до цього часу відсутнє спеціальне комплексне дослідження правосуб'єктності фізичної особи в мережі «Інтернет». Означене є свідченням необхідності проведення комплексного дослідження специфіки правосуб'єктності фізичної особи в мережі «Інтернет» з огляду на вплив автономних систем прийняття рішення, профілювання, безперервної обробки персональних даних на концепцію новітнього покоління цифрових прав людини, що обґрунтовує значущість та актуальність обраної теми.

Тому актуальність обраної теми дисертаційного дослідження зумовлюється необхідністю розвитку науки цивільного права стосовно правосуб'єктності фізичної особи в мережі «Інтернет», удосконалення чинного законодавства України в даній сфері, та практики його застосування.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконана відповідно до плану науково-дослідної роботи кафедри права інтелектуальної власності та патентної юстиції Національного університету «Одеська юридична академія» «Людиноцентристський підхід у забезпеченні прав інтелектуальної власності в цифрову добу» на 2021-2025 роки як складової плану науково-дослідної роботи Національного університету «Одеська юридична академія» «Правове та соціальне життя людини в людиноцентристському вимірі в цифрову еру» на 2021-2025 рр. (державний реєстраційний номер 0122U000266).

Мета і завдання дослідження. Метою дисертаційного дослідження є розв'язання наукової проблеми, обумовленої потребою встановлення особливостей правосуб'єктності фізичної особи у відносинах у мережі «Інтернет», переосмислення уявлень щодо розуміння фізичної особи під впливом розвитку інформаційно-комунікаційних технологій, виявлення впливу

мережі на зміст правосуб'єктності фізичної особи, особливості виникнення та припинення правоздатності та дієздатності, з формулюванням відповідних теоретичних та практичних рекомендацій, спрямованих на вдосконалення цивілістичної доктрини та практики її здійснення.

Для досягнення зазначеної мети в дисертації були розв'язані такі завдання:

- розглянути концептуальні підходи до розуміння мережі як чинника, який впливає на уявлення про людину в мережі «Інтернет»;
- запропонувати наукові підходи до визначення права на цифрову ідентичність у мережі «Інтернет»;
- розглянути наукові підходи до визначення цифрової ідентичності фізичної особи в мережі «Інтернет»;
- дослідити специфіку проведення ідентифікації та ідентифікуючих ознак фізичної особи у відносинах у мережі «Інтернет»;
- визначити специфіку виникнення та припинення правоздатності та дієздатності фізичної особи в мережі «Інтернет»;
- проаналізувати зміст цивільної правоздатності фізичної особи в мережі «Інтернет»;
- розглянути особисті немайнові права у складі цивільної правоздатності фізичної особи в мережі «Інтернет»;
- дослідити специфіку дієздатності фізичної особи у відносинах у мережі «Інтернет»;
- розробити науково-теоретичні пропозиції та практичні рекомендації

у сфері правового регулювання правосуб'єктності фізичної особи у відносинах у мережі «Інтернет».

Об'єктом дослідження є правовідносини, що складаються стосовно реалізації правосуб'єктності фізичної особи в мережі «Інтернет».

Предметом дослідження є правосуб'єктність фізичної особи у відносинах у мережі «Інтернет».

Методи дослідження обрані з урахуванням поставленої мети та завдань досліджень. Методологічну основу дисертаційної роботи склали

загальнонаукові та спеціальні методи пізнання. Провідним загальнонауковим методом дослідження є діалектичний метод, який допоміг простежити формування концепції цифрової ідентичності фізичної особи в мережі «Інтернет» у тісному взаємозв'язку з економічними, політичними та соціальними процесами, з урахування широкого та вузького розуміння категорії «цифрова ідентичність», дослідити процедуру ідентифікації та засобів ідентифікації фізичної особи в мережі «Інтернет» (підрозділи 1.1, 1.2, 2.1, 2.3, 2.4). Істотну роль у проведенні дослідження відіграв порівняльний метод, за допомогою якого проведено порівняльний аналіз зарубіжного законодавства у виборі підходів до правового регулювання цифрової ідентичності фізичної особи в мережі «Інтернет», доступу до акаунту фізичної особи у мережі після її смерті, цифрових прав людини у зв'язку із використанням коду як регулятора відносин у мережі, проаналізувано підходи до правового положення інтелектуальних автономних агентів, порівняти підходи до розуміння окремих цифрових прав у законодавстві та судовій практиці окремих держав ЄС та США (підрозділи 2.2, 3.2, 3.3, 3.4). Метод системного-структурного аналізу дозволив розглянути поняття та сутність цифрової ідентичності в широкому та вузькому розумінні, сутність та властивості цифрових прав, які складають зміст правоздатності фізичної особи, (підрозділи 2.2, 3.2, 3.3). Використання формально-логічного методу дозволило удосконалити визначення деяких категорій, які мають істотне значення для формування концепції правосуб'єктності фізичної особи, зокрема запропоновані уточнення стосовно розуміння цифрової ідентичності в широкому та вузькому значенні, визначення біометричних даних та розуміння виникнення та припинення прав та обов'язків у мережі «Інтернет» (підрозділи 2.1, 2.3, 3.1). Використання методу аналізу та синтезу дозволило визначити категорію цифрова ідентичність фізичної особи в широкому та вузькому розумінні, розкрити зміст правоздатності та дієздатності фізичної особи в мережі «Інтернет», з'ясувати специфіку новітніх прав, обумовлених розвитком інноваційних технологій, сформулювати висновки на підставі проведених наукових пошуків (підрозділи 2.1, 3.2, 3.3, 3.4). Синергетичний метод сучасних

правових досліджень дозволив змоделювати вектори розвитку майбутніх цивільних відносин за участі фізичної особи та формування концепції цифрової ідентичності фізичної особи в мережі «Інтернет» з урахуванням розвитку автоматизованих систем та інтелектуальних програмних агентів (підрозділи 1.1, 1.2, 2.2).

Теоретичну основу дисертаційного дослідження склали наукові праці вітчизняних та зарубіжних науковців у сфері загальнотеоретичної юриспруденції, конституційного, інформаційного, цивільного права та інших галузей системи права України, зокрема у сфері економіки, соціології та філософії.

Нормативно-правову основу дисертаційного дослідження склали Конституція України, міжнародно-правові акти, акти цивільного законодавства України та окремих зарубіжних держав.

Емпіричну базу дисертаційного дослідження становлять рішення Європейського суду з прав людини, Суду ЄС, Верховного Суду України, місцевих судів загальної юрисдикції, судів іноземних держав (США, Великобританія, Франція, Німеччини).

Наукова новизна одержаних результатів полягає в тому, що дисертація є першим у вітчизняній науці цивільного права комплексним дослідженням теоретичних та практичних проблем правосуб'єктності фізичної особи у відносинах у мережі «Інтернет». Наукова новизна одержаних результатів знайшла своє відображення в таких наукових положеннях:

вперше:

запропоновано розрізняти цифрову ідентичність фізичної особи в інтернеті у широкому та вузькому значеннях. Цифрова ідентичність у вузькому значенні – цифровий образ суб'єкта цивільних відносин (джерело персональних даних особи, акаунт (обліковий запис), який ідентифікує його у відповідних системах). Цифрова ідентичність у широкому значенні – це система даних суб'єкта цивільних правовідносин, без прив'язки до конкретного акаунта, в тому числі всі

дані, які особа залишає у результаті активної та пасивної діяльності, за винятком даних, які не дозволяють ідентифікувати особу;

доведено, що підхід до цифрової ідентичності у вузькому та широкому значеннях проявляться у спадкових відносинах та доступі до цифрової спадщини після смерті фізичної особи;

запропоновано розуміння права на цифрову ідентичність як особистого немайнового права, обумовленого розвитком технологій, що належить кожній фізичній особі, є комплексним за своєю структурою і складається з права на визнання цифрової ідентичності, права перешкоджати будь-якому спотворенню та посяганню на цифрову ідентичність, яке здатне завдати шкоди фізичній особі;

доведено, що цифрова репутація як особисте немайнове благо в умовах розвитку соціальних мереж, шерингових платформ виходить за межі лише суспільної оцінки ділових, професійних якостей та здібностей фізичної особи, а пов'язується з якостями та оцінками особи, які персоніфікують її не лише поміж фахівців у галузі, а й решти користувачів цифрового середовища, безпосередньо впливає на можливість участі у комунікації, договірних відносинах, отриманні прибутку як в мережі «Інтернет», так і у фізичному світі;

обґрунтовано, що момент виникнення правоздатності фізичної особи в мережі «Інтернет» залежить від підходу держав до правового регулювання відносин в інтернеті. Здійснення прав в мережі «Інтернет» може істотно варіюватися залежно від механізмів правового регулювання здійснення прав та обов'язків користувачів та обраного державою підходу: ліберального – властивого західному підходу (ЄС, США) або авторитарного – властивого закритому, східному підходу регулювання інтернету (КНР);

доведено, що внаслідок смерті фізичної особи відбувається трансформація цифрової ідентичності, перехід прав на цифрове майно та отримання спадкоємцями доступу до акаунтів особи в інтернеті. Встановлено, що видалення акаунту та персональної інформації користувача, а з тим і здійснення фізичною особою своєї правоздатності та дієздатності у мережі, може бути добровільним (за волевиявленням фізичної особи) і примусовим та застосовуватися в якості

санкції за вчинення правопорушення за рішенням суду або порушення умов користувацької угоди за рішенням інтернет-сервісу. Користувач має право залишити розпорядження на цифровій платформі на випадок смерті, відносно долі цифрових речей, призначити осіб, яким має бути наданий доступ або розпорядитися про видалення акаунту;

запропоновано поняття цифрової смерті як правової категорії – це видалення акаунту за життя людини або трансформація акаунту у цифровий меморіал у разі її смерті. Категорія цифрової смерті може не співпадати з категорією смерті фізичної особи;

запропоновано передбачити у законодавстві право суб'єктів даних на отримання інформації про логіку прийнятого індивідуального рішення (аналізу вхідних даних, статистичного пояснення, перевірки коду, визначення чутливості окремих даних та змінних, які зумовили результат) та кореспондуючий обов'язок контролера у разі прийняття рішення із застосуванням алгоритму надати інформацію суб'єкту даних про логіку індивідуального рішення, що лежить в основі обробки;

запропоновано до системи цифрових прав включити право бути обізнаним про використання автоматизованих систем у прийнятті юридично значущих рішень та надати право суб'єктам даних оскаржувати юридично значущі рішення, які прийняті за участі автоматизованих систем;

доведено, що суб'єкти прийняття юридично значущих рішень схильні надмірно покладатися на рішення автоматизованих систем, ігноруючи власні судження, тому остаточне рішення повинно ухвалюватися людиною;

доведено, що у таких сферах, як фінанси та судочинство попереднє рішення автоматизованої системи може тягти для суб'єкта даних несприятливі наслідки, суттєво обмежувати у здійсненні прав, затаврувати в суспільстві, внаслідок того, що суб'єкт прийняття юридично значущого рішення надає йому першочергового значення у своїй процедурі ухвалення рішення;

запропоновано розрізняти види упереджень, які впливають на прийняття юридично значущих рішень із використанням автоматизованих систем: 1)

структурні упередження, які виникають внаслідок програмування системи; 2) упередження в даних унаслідок функціонування системи, яка виводить певне значення у рівень еталону (нерепрезентативні дані); 3) алгоритмічні упередження, обумовлені тим, що суб'єкт надмірно покладається на рішення, прийняті алгоритмом, нехтуючи критичним мисленням;

доведено, що право на роз'яснення та обґрунтування прийняття конкретного автоматизованого юридично значущого рішення не забезпечено гарантіями, передбаченими ст. 22, та обов'язками контролерів надати доступ до даних згідно зі ст. 13, 14 Регламенту ЄС 2016/679;

доведено, що внаслідок цифрового профілювання створюються нові дані, які не є ідентичними тим, що були надані суб'єктом даних, а метод профілювання створює значні ризики для прав та свобод людини, коли людина може потрапляти в певні категорії, не знаючи про це. Профілювання може призводити до обмеження доступу до певних товарів та послуг, створювати дискримінацію та підвищувати ризики втручання у приватне життя;

для недопущення зловживання генетичними технологіями та дотримання прав людини, запропоновано доповнити: статтю 99 Закону України «Про страхування» положенням про заборону оцінки ризику на основі прогностичного генетичного тестування, заборону страховиків вимагати проходження генетичного тестування та запитувати у застрахованих осіб або родичів надання результатів такого тестування; статтю 2-1 Кодексу законів про працю України положенням про заборону вимагати від працівників проходження генетичного тестування, подання його результатів, іншої інформації щодо генетичних особливостей працівника (його родичів) та будь-яку дискримінацію за генетичними ознаками;

вдосконалено:

визначення біометричних даних в частині визнання персональних даних біометричними даними через застосування спеціальної технічної обробки фізичних, фізіологічних або поведінкових характеристик особи, з метою однозначної ідентифікації фізичної особи;

розуміння цифрових прав як прав людини нового покоління та включення до їх числа, поряд із загальновизнаними правами людини, які здійснюються в мережі «Інтернет», прав, обумовлених функціонуванням технологій (право на доступ до даних, на видалення даних, виправлення та уточнення даних, на перенесення даних, обмеження обробки даних, заперечення проти обробки та проти прийняття значущого рішення на підставі автоматизованої обробки персональних даних та інші), та здійснення яких може забезпечуватись, разом із правовими засобами, програмним кодом;

розуміння права доступу до інтернету як похідного від права на інформацію (здійснення права доступу до інфраструктури мережі «Інтернет» та до контенту), що вимагає від держав виконання позитивних (забезпечення підключення до мережі, якщо в місцевості відсутня необхідна інфраструктура) та негативних гарантій (невтручання у приватне життя, недопустимість масового обмеження доступу та блокування до ресурсів, недопущення переслідування користувачів на підставі політичних переконань та поглядів у мережі «Інтернет»);

зміст права на інформаційну приватність, як особистого немайнового права особи контролювати обсяг та зміст інформації, пов'язаної зі збором та обробкою персональних даних. Вдосконалено визначення права на інформаційну приватність, в частині доповнення правомочностями вимагати від контролерів виконання їх обов'язків щодо здійснення суб'єктом його прав: на доступ, уточнення, перенесення, обмеження обробки, видалення персональних даних; заперечувати проти обробки та обмеження обробки персональних даних із застосуванням автоматизованих систем; вимагати захисту порушених прав;

дістало подальшого розвитку:

підхід щодо віднесення даних до персональних, з урахуванням розуміння персональних даних, передбаченого Регламентом ЄС 2016/679, що ґрунтується на оцінці ризику ідентифікації суб'єкта даних, а не на можливості ідентифікації особи як такої. За такого підходу дані, які є персональними, можуть бути визнані не персональними даними у разі, якщо ідентифікація особи за їх допомогою

невигідна або недоцільна, оскільки потребує непропорційно великих витрат на обробку, забезпечення безпеки для контролера**;**

теза, що при визначенні правової ідентифікації суб'єктів даних під час обробки даних автоматизованими системами, контролери змушені приймати до уваги проведення конкретної та ймовірнісної ідентифікації. Доведено необхідність розмежування даних, які допускають та не допускають конкретну ідентифікацію особи. Під неможливістю конкретної ідентифікації розуміється «ймовірнісна ідентифікація», яка на основі аналізу великих даних, за окремими ознаками, не дозволяє конкретно ідентифікувати особу або у поєднанні із інформацією про поведінку (дії) особи, призводить до ідентифікації. Імовірнісна ідентифікація може відбуватися під час застосування окремих видів кукі файлів;

висновок, що право на доступ до персональних даних є умовою для здійснення інших прав суб'єктів даних. Обґрунтовано, що з урахуванням судової практики та законодавства ЄС, право на доступ до персональних даних може бути передумовою для ефективного здійснення права на виправлення даних, заперечення проти обробки, звернення до суду та третіх осіб для отримання компенсації;

положення про право на доступ до персональних даних. З урахуванням судової практики та законодавства ЄС, доведено, що контролер має надати суб'єктам даних інформацію про одержувачів у разі несанкціонованого розголошення даних (витоку), за винятком неможливості їх ідентифікувати або у разі явно необґрунтованого або надмірного запиту суб'єкта даних, розкрити категорії відповідних отримувачів, не розкриваючи фактичних осіб;

положення про здійснення права на уточнення даних. Обґрунтовано, що фізична особа може здійснити право на уточнення для доповнення, виправлення неповної інформації як у первинних даних, так і у разі неточних результатів профілювання. Контролер має право відхилити надані суб'єктом уточнюючі персональні дані лише у випадку, якщо вони не відповідають меті його обробки;

теза про те, що здійснення права бути забутим не є абсолютним. Доведено, що право на забуття не застосовується, коли обробка персональних даних

необхідна для: здійснення права на свободу вираження думки та свободу інформації; виконання завдань в інтересах суспільства або при виконанні офіційних повноважень, покладених на контролера суспільних інтересів у галузі охорони здоров'я; архівування у суспільних інтересах, наукових та історичних дослідженнях, статистичних та інших подібних цілей; здійснення судочинства. Здійснення права на забуття може полягати у видаленні посилання на публікацію у пошуковому запиті;

теза про необхідність встановлення стандартів функціонування систем ШІ та їх дотримання компаніями. Обґрунтовано необхідність інформування суб'єктів про використання автоматизованих систем у товарах, послугах та про право бути поінформованими про взаємодію саме з агентом ШІ, а не людиною. Інформування суб'єктів про використання автоматизованих систем може здійснюватися шляхом маркування товарів, робіт, публікацій (у разі внесення змін в новини, фото та відео) для запобігання введення суб'єктів в оману;

теза, що розвиток систем ШІ має відбуватися на принципах відповідальності, підзвітності, антропоцентричності та заслуговуючих довіри систем ШІ. Зроблено висновок, що з метою дотримання прав фізичних осіб у захисті недоторканності приватного життя та врахування публічних інтересів, необхідно передбачити у законодавстві: 1) заборону використання технології віддаленої біометричної ідентифікації «в режимі реального часу»; 2) заборону невибіркової ідентифікації та прихованого відеоспостереження; 3) заборону використання систем соціального рейтингу (оцінки); 4) заборону використання технологій впливу на підсвідомість для маніпулювання, підбурювання до певної поведінки та прийняття рішень; 5) заборону проведення невибіркового або нецільового розпізнавання обличчя шляхом розширення баз даних за рахунок зображень облич із мережі «Інтернет», приватних баз даних та створення об'єднаних баз;

теза про необхідність запровадження в проєкті Закону України «Про єдину систему відеомоніторингу стану публічної безпеки» етапів застосування технології. Запропоновано, з метою забезпечення прозорості застосування

дистанційної біометричної ідентифікації передбачити такі етапи: 1) формування бази даних фото (із біометричним шаблоном); 2) отримання зображень обличчя з камер відеоспостереження; 3) розпізнавання облич програмою; 4) вилучення унікальних ознак з зображення кожного обличчя та створення біометричних шаблонів; 5) порівняння обличчя (програма порівнює вилучені рис обличчя із зображеннями облич, у базі даних); 6) встановлення співпадіння (програма обчислює ступінь співпадіння). Якщо ступінь співпадіння є вищим за встановлену межу, дані передаються для подальшої обробки фізичній особі для підтвердження (або спростування) співпадіння та вжиття заходів перевірки суб'єкта уповноваженими органами (посадовими особами). Якщо співпадіння не виявлено, відео, які надійшли з камери спостереження, підлягають видаленню у строк, передбачений законом;

твердження про те, що забезпечення балансу між конкуруючими інтересами осіб, чиї дані обробляються, та інтересами суспільства, потребує дотримання засад «необхідності» щодо обробки персональних даних. Обґрунтовано, з урахуванням судової практики та законодавства ЄС, що обробка персональних даних, використання технологій віддаленої біометричної ідентифікації можуть застосовуватися лише у разі суворої «необхідності», яка свідчить про неможливість досягнення контролером мети законної обробки іншим шляхом. Необхідність має бути наявною, реально існуючою або вона має виникнути в найближчому майбутньому, а не гіпотетичною;

теза про застосування законодавства про агентські відносини до автономних інтелектуальних систем (програм). При цьому застування законодавства про агентські відносини доцільне у разі завантаження (активації) ліцензіатом програмного забезпечення та покладення відповідальності за шкоду на ліцензіатів або користувачів (як осіб, які набули використання виключними правами на об'єкт) у договірних відносинах. У деліктних відносинах відповідальність за дії агента поряд із принципалом може покладатися субсидіарно на розробника програмного забезпечення (страхову компанію).

Практичне значення одержаних результатів полягає в тому, що висновки і пропозиції, сформульовані в дисертації, можуть бути використанні у:

науково-дослідній діяльності – як основа для подальшого наукового дослідження цивільно-правових проблем категорії правосуб'єктності та статусу фізичної особи в умовах розвитку інформаційно-комунікаційних технологій та інтернету;

правотворчій діяльності – у процесі вдосконалення норм цивільного законодавства щодо змісту правоздатності та дієздатності прав та обов'язків, захисту порушених прав фізичної особи, гармонізації національного законодавства та адаптації правових основ регулювання до європейських стандартів;

правозастосовній сфері – у практиці органів юстиції (Акт про впровадження результатів дисертаційного дослідження в діяльність Південного міжрегіонального управління Міністерства юстиції (м. Одеса), при розгляді судами цивільних справ, що стосуються прав, обумовлених розвитком мережі «Інтернет» та автоматизованих систем (Акт про впровадження результатів дисертаційного дослідження у практичну діяльність Київського суду м. Одеси), у практичній діяльності приватних виконавців (лист про впровадження результатів дисертаційного дослідження в діяльність приватних виконавців Одеської області), у практичній діяльності нотаріуса (лист приватного нотаріуса Одеського міського нотаріального округу);

у навчальному процесі – при викладанні навчальних дисциплін «Цивільне право», «Цивільне та сімейне право», «Захист персональних даних» та ін., розробці навчальних планів і програм, підготовці підручників, навчальних посібників, практикумів із зазначених дисциплін (Акт про впровадження результатів дисертації в навчальному процесі Національного університету «Одеська юридична академія»); при викладанні навчальних дисциплін «Актуальні проблеми права інтелектуальної власності» та «Приватне право: практика тлумачення та правозастосування», розробці навчально-методичних матеріалів (Акт про впровадження результатів дисертаційного дослідження в

освітній процес Одеського державного університету внутрішніх справ); при викладанні лекційних занять з дисциплін «Цивільне право», «Право інтелектуальної власності», «Цивільно-правовий захист особистих немайнових прав» (Акт про впровадження результатів дисертації в наукову діяльність Хмельницького університету управління та права імені Леоніда Юзькова).

Особистий внесок здобувачки. Дисертація є самостійним науковим дослідженням, теоретичні положення, висновки та пропозиції сформульовані в дисертації, отримані авторкою самостійно.

У співавторстві з дисертанткою опубліковані такі наукові праці: Nekit K., Tokareva V., Zubar V. Artificial intelligence as a potential subject of property and intellectual property relations. *Ius Humani. Law Journal.* 2020. № 9 (1). P. 231-250. (особистий внесок: дослідження можливості штучного інтелекту виступати суб'єктом права інтелектуальної власності); Tokareva V. Davydova I., Adamova E. Legal problems of the use of orphan works in digital age. *Juridical Tribune.* 2021. № 11. P. 453-471. (особистий внесок: дослідження перешкод вільної реалізацію права на творчість в умовах цифоровізації та перспектив правового регулювання сирітських творів, висновки щодо впливу цифровізації на вираження творчості та легалізацію сирітських творів в мережі Інтернет); Davydova I., Zhurylo S., Tomina V., Fuchedzhi V., Tokareva V. Legal aspects of the regulation of social relations with the participation of Artificial Intelligence. *Revista De La Universidad Del Zulia.* 2022. № 38. P. 487-500. (особистий внесок: визначення теоретичних основ та доктрини регулювання суспільних відносин за участю штучного інтелекту, висновок, щодо позиціонування роботів зі штучним інтелектом як окремих об'єктів правовідносин, в тому числі як можливих суб'єктів правовідносин); Davydova, I., Nahnybida, V., Adamova, O., Zhurylo, S., & Tokareva, V. Blockchain and civil proceedings: points of convergence. *DIXI.* 2022 (2023). № 25(1). P. 1–20. (особистий внесок: дослідження джерел щодо використання технології блокчейн у держаному управлінні та судочинстві, як засобу регулювання відносин за допомогою програмного коду, висновок, щодо можливості застосування технології блокчейн для вирішення проблем

судочинства); Davydova I., Bernaz-Lukavetska O., Tokareva V., Andriienko I., Tserkovna O. Freedom of contract in the digital age and its implementation in modern technologies: theory and practice. *International Journal of Computer Science and Network Security*. 2022. № 12. P. 544-548. (особистий внесок: визначення перспектив використання смарт контрактів та регулювання відносин за допомогою програмного коду в умовах цифровізації); Давидова І.В., Токарева В.О. Захист права на повагу до честі та гідності, ділової репутації, публічних осіб. *Держава та регіони. Серія Право.* 2022. № 1 (75). С. 131-135. (особистий внесок: дослідження теорії та правозастосовчої практики ЄСПЛ щодо захисту права на повагу честі та гідності, ділової репутації публічних осіб); Токарева В.О., Личко В.С**.** Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С. 848-851. (особистий внесок: дослідження практики та доктринальних підходів правового врегулювання надання доступу до цифрових об'єктів у Франції та Іспанії); Токарева В.О., Личко В.С. Спадкування об'єктів у мережі «Інтернет»: досвід західних держав. *Часопис цивілістики.* 2024. № 53. С. 41-46. (особистий внесок: теоретичне дослідження практики та доктринальних підходів правового врегулювання надання доступу до об'єктів у мережі «Інтернет» після смерті спадкодавця в США); Давидова І.В., Токарева В.О. Цифрова нерівність і право на доступ до інтернету. *Юридичний вісник.* 2024. № 6. С. 68-75. (особистий внесок: теоретичний аналіз правового регулювання щодо забезпечення здійснення права на рівний доступ до мережі «Інтернет», висновок щодо визнання доступу до Інтернету в якості права людина).

Апробація результатів дослідження. Результати дослідження обговорено на засіданнях кафедри цивільного права та кафедри права інтелектуальної власності і патентної юстиції Національного університету «Одеська юридична академія» та на засіданні Південного регіонального центру НАПрН України. Основні положення дисертації були апробовані на 31 науковому заході, а саме: Міжнародній науково-практичній конференції «Розвиток державності та права в Україні реалії та перспективи» (м. Львів, 20 вересня 2019 р.); Всеукраїнському

круглому столі «Інформаційні технології в умовах оновлення цивільного законодавства» (м. Одеса, 13 червня 2020 р.); Міжнародній науково-практичній конференції «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру» (м. Одеса, 21 травня 2021 р.); Міжнародній науково-практична конференція (м. Київ, 22 червня 2021 р.); Міжнародній науково-практичній конференції Юридична наука: виклики і сьогодення» (м. Одеса, 11 червня 2021 р.); Міжнародній науково-практичній конференції «Сучасне правотворення: питання теорії та практики» (м. Дніпро, 4 червня 2021 р.); Міжнародній науково-практичній конференції «Особливості розвитку законодавства України у контексті євроінтеграційних процесів» (м. Харків, 4 червня 2021 р.); Міжнародній науково-практичній конференції «Сучасний вимір держави і права» (м. Львів, 18 червня 2021 р.); Міжнародній науково-практичній конференції «Актуальні питання реформування правової системи України» (м. Дніпро, 2 липня 2021 р.); Міжнародній науково-практичній конференції «Актуальні питання правової теорії та юридичної практики» (м. Одеса, 13 серпня 2021 р.); Міжнародній науково-практичній конференції «Проблеми та стан дотримання і захисту прав людини в України» (м. Львів, 20 серпня 2021р.); Міжнародній науково-практичній конференції «Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (м. Одеса, 17 червня 2022 р.); Міжнародній науково-практичній інтернет-конференції «International Scientific and Practical Internet Conference «Integration of Education, Science and Business in Modern Environment» (м. Дніпро, 15 серпня 2022 р.); Всеукраїнській науково-практичній конференції «Розвиток громадянського суспільства як необхідна складова європейської інтеграції України» (м. Київ, 6 жовтня 2022 р.); Міжнародній науково-практичній конференції «Правове регулювання суспільних відносин: перспективні напрями на шляху до сталого розвитку» (м. Київ, 28 жовтня 2022 р.); Всеукраїнській науковій конференції «Приватне право в умовах війни» (м. Одеса, 15 листопада 2022 р.); 12th International Conference Challenges of Business Law in the Third Millennium (Bucharest, 25 November 2022); Міжнародній

науково-практичної конференції, присвяченій 102-річчю Національного університету кораблебудування імені адмірала Макарова «Становлення та розвиток правової держави: проблеми теорії та практики» (м. Миколаїв, 28 грудня 2022 р.); Міжнародній науково-практичній конференції «Актуальні проблеми протидії корупції в Україні в умовах воєнного стану» (м. Рівне, 14 березня 2023 р.); Міжнародній науково-практичній конференції Таврійського національного університету до 160-ї річниці від дня народження В. І. Вернадського (м. Київ, 16 березня 2023 р.); International scientific conference «Topical issues of modern jurisprudence»: conference proceedings (Częstochowa, 5 April 2023); Всеукраїнській науково-практичній конференції «Гармонізація законодавства України з правом Європейського Союзу: реалії та перспективи» (м. Запоріжжя, 18 травня 2023 р.); Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень» (м. Одеса, 19 травня 2023 р.); Всеукраїнській науково-практичній конференції «Римське право і сучасність: актуальні проблеми оновлення цивільного законодавства» (м. Одеса, 25 травня 2023 р.); Круглому столі «Проблеми цивільного права у постпандемічну добу» (м. Одеса, 26 травня 2023 р.); International scientific conference «Legal science, legislation and law enforcement: traditions and new European approaches» (Wloclawek, 29 May 2023); Міжнародній науково-практичній конференції «Восьмі Таврійські юридичні наукові читання» (м. Київ, 16 червня 2023 р.); Круглому столі «Цивілістичні проблеми спортивного права» (м. Одеса, 28 жовтня 2023 р.); Всеукраїнській науковій конференції «Договори в умовах миру та війни (до 90-річчя з дня народження В. Луця)» (м. Одеса, 1 грудня 2023 р.); Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів» (м. Одеса, 26 квітня 2024 р.); Всеукраїнській науковій конференції «Римське право і сучасність: реалізація і захист речових прав в умовах воєнного стану» (м. Одеса, 25 травня 2024 р.); Всеукраїнській

науковій конференції «Одеські грудневі цивілістичні читання: приватне право, як концепт в умовах війни, людський вимір» (м. Одеса, 12 грудня 2024 р.).

Публікації. Основні положення та результати дисертації відображено у 73 публікаціях, 27 наукових статтях, опублікованих у фахових виданнях, перелік яких затверджено МОН України, з яких 4 у співавторстві, 9 наукових статтях, опублікованих у зарубіжних періодичних виданнях з юридичного напрямку, зокрема 5 статтях проіндексованих у базах даних Web of Science Core Collection та/або Scopus, 31 тезах доповідей на науково-практичних конференціях, засіданнях круглих столів.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, які містять 10 (з яких один поділений на пункти) підрозділів, висновків, списку використаних джерел (888 найменувань) та додатків. Загальний обсяг роботи – 529 сторінок, з яких основного тексту – 390 сторінок.

1. ГЕНЕЗИС ТА ЮРИДИЧНА ПРИРОДА ФІЗИЧНОЇ ОСОБИ В МЕРЕЖІ «ІНТЕРНЕТ»

1.1. Вибір напрямів дослідження

Спосіб життєдіяльності людини радикально змінюється під впливом VR та AR, коли «людина суспільна» перетворюється на «людину інформаційну», змінюється спосіб, яким вбачається світ, у реальному та соціальному просторі. Розуміння можливостей формування суб'єктності агентів соціальної дії та комунікації дозволяє визначити напрями трансформації людини та напрями, які визначають подальші зміни в суспільстві.

Наразі людина та її правове існування поступово переходить з фізичної реальності у VR, яка отримує правове регулювання попри позиції прибічників вільного інтернету (особливо через соціальну значущість дій та правочинів у мережі). Процес правового впорядкування віртуального середовища є об'єктивним та продовжує зростати в масштабах, через посилення цифровізації соціального середовища.

У літературі поряд із терміном – «цифровізація» [193], використовується – «діджиталізація» [122, с. 297] в різних значеннях. М.С. Міхровська з цього приводу стверджує, що «діджиталізація» є синонімом «оцифрування» в перекладі з англійської мови [106]. Обидва терміни, за визначенням О.Б. Бутнік-Сіверського, позначають переведення інформації в цифрову форму, тобто зміну форми документів з фізичної в цифрову, або відмову від паперових носів для переміщення на екран комп'ютера, або навпаки [16, с. 94]. Оцифрування ефективно використовується для збереження даних у різних сферах [828, с. 452; 222, с. 107; 223, с. 197; 224, с. 97].

Наразі відбувається оцифрування та віртуалізація всього буття, що зумовлює гібридизацію реального та віртуального життя, можна сказати участь людини у двох «протилежних світах». Означене сприяє поступовому стиранню межі між онлайн та офлайн, реальністю та віртуальністю. Цей процес призводить до трансформації традиційних антропологічних складових: особа поступово

перестає бути виключно тілесною істотою, а до її єдності додається цифрова компонента, поряд із біологічною та соціальною. Так людина та кожен із компонентів свідомості, волі та здатність до діяльності переживає зміни в цифровому середовищі.

Упродовж значного періоду людина могла створювати необмежену кількість цифрових образів, цифрових профілів під різними іменами, які не збігалися з фізичною особою в реальному світі. Слід навести висловлювання Д. Коупленда: «Ви – це не Ваше тіло» [444, с. 55], яке у віртуальному середовищі може означати відсутність прямого взаємозв'язку між фізичною особою та цифровим профайлом: жінка може видавати себе за чоловіка, дитина – за дорослого тощо [570, с. 43]. Прихильники концепції інтернет-суспільства відстоюють важливість збереження ключових характеристик кіберпростору як середовища, вільного від обмежень, зумовлених фізичними та культурними нормами, дозволяючого створювати цифрові образи, яким людина прагне, проте є відмінними від фактично існуючих у фізичному світі [870, с. 145].

Унаслідок цього виникає мультиплікаційний ефект цифрових технологій, коли кількість цифрових профілів, цифрових ідентичностей у мережі «Інтернет» перевищує кількість фізичних осіб у реальному світі (навіть якщо брати до уваги, що значна кількість населення не використовує новітні технології). У зв'язку з тим, що ефект мультиплікації та множинність акаунтів, які наразі зберігаються в мережі «Інтернет», подекуди може спричиняти негативні наслідки для неповнолітніх та необхідність припинення вчинення протиправних дій суб'єктами, GAFAM запроваджує технічні заходи та політику єдиної автентичної ідентичності (надалі буде розглянуто в Підрозділі 2.2. «Формування концепції цифрової ідентичності фізичної особи в мережі «Інтернет»).

На первісному етапі розвитку інтернету провідною особливістю впливу інтернету на фізичну особу називалася можливість вільного вибору ідентичності в мережі [665, с. 159]. Визнаючи вагомий вплив глобалізації на сучасне буття, філософи розглядають сучасну людину, як новий антропологічний вид, життя якої вбудовується в умовах підривних інновацій, що стрімко змінюють світ.

Слід зазначити, що необхідно відрізняти людину як біологічну істоту від уявлень людини в законодавстві, тобто від фізичної особи. Ці поняття пов'язані між собою, але не є тотожними.

Римські юристи використовували термін persona в широкому та вузькому розумінні. У широкому значенні (біологічному), persona застосовувалася як синонім для позначення людини як живої істоти, а у вузькому, суто юридичному значенні, як «особа» для характеристики людини як суб'єкта права.

Оскільки людина сама по собі не є суб'єктом права, це робиться завдяки юридично організованими інститутами громадянського суспільства [692, с. 84]. Так, ст. 24 ЦК України передбачає, що людина як учасник цивільних відносин вважається фізичною особою.

Є.О. Харитонов та О.І. Харитонова зазначають, що відмінність між цими категоріями полягає в тому, що поняттям «людина» охоплюється будь-яка біопсихосоціальна істота, незалежно від того, чи вступає вона в цивільні відносини, чи ні. Натомість «фізичною особою» є людина як суб'єкт цивільних відносин. Разом із тим, людина може бути, а може й не бути учасником цивільних відносин, вона може бути суб'єктом права, а може розглядатися як об'єкт впливу в іншій системі суспільних зв'язків. Таким чином, поняття фізичної особи в цивілістиці може не збігатися з поняттям людини як істоти біологічної: іноді ці поняття тотожні, а іноді – поняття «фізична особа» вужче поняття «людина». Разом із тим, поняття «фізична особа» та «людина» розглядаються як кореляти [261, с. 142].

У свою чергу, англомовні джерела використовують термін individual або natural person, який перекладається як індивід або фізична особа. Дані терміни протиставляються категорії «юридична особа», яка позначається терміном – legal person або legal entity, або legal personhood [754, с. 101.], [677]. Термін natural person або «фізична особа» використовується як юридична концепція для позначення живої людини або людської істоти, як особи [678], [680], яка визнається правом [604]. Саме «natural person» або «personne physiqu», або

«фізична особа» визнається суб'єктом права за французьким правом [679] та наділяється правами та обов'язками [681].

Таким чином, категорія «особа» накопичила значні традиції наукової думки і займає центральне місце у філософії, суспільстві та праві. Поряд із цим, у цифровому середовищі на перший план виходить система даних фізичної особи в інтернеті, що змушує філософів, соціологів до переосмислення та пропонування пропозицій використання різних категорій та понять щодо фізичної особи в мережі «Інтернет», які будуть розглянуті далі. Тому доцільно звернутися до соціології та філософії, які пропонують власні підходи та термінологічний апарат для розуміння фізичної особи у відносинах у мережі «Інтернет» та впливом інформаційно-комунікаційних технологій.

Французькі філософи-постмодерністи Жорж Батай, Жіль Дельоз і Жан Бодрійяр для позначення образу, який не має оригіналу або який втратив його з часом, пропонували застосовувати термін «симулякр». Симулякр описує розуміння багатьох сучасних процесів, які наразі відбуваються – від постмодерністського мистецтва до віртуальної реальності. Не випадково в «Матриці» герой Кіану Рівза використовує як схованку книгу французького філософа Жана Бодрійяра «Симулякри та симуляція». Адже, по суті, матриця – і є симулякра, тобто копія чогось, що не існує насправді. Комп'ютерна програма відтворює світ, який давно зник у кінці XX сторіччя [262, с. 9].

Термін «симулякр» вперше вживається в латинських перекладах Платона – як еквівалент грецького «ейдолон». Грецький філософ розділяв матеріальний світ та трансцендентний світ ідей – ейдосів. Ідеї втілюються в реальних предметах та важливо, щоб ці втілення відбувалися без спотворень. «Ейдолон» є хибною копією, що спотворює ідею первісного образу, не відображає його сутності, тому порушує гармонію Всесвіту.

На думку Ж. Дельоза людина і є симулякром, що Бог створив людину за образом та подобою. Однак у результаті гріхопадіння людина втратила подобу до Бога, зберігаючи при цьому образ. Дотримуючись такого твердження, людина є симулякром, відмовляється від морального існування задля того, щоб увійти до

стадії естетичного існування. Ж. Дельоз визначає симулякр як копію копій, нескінченно деградовану ікону, подобу, із якою втрачається істотне, різниця у природі між симулякром і копією. Копія є образом, наділеним схожістю, симулякр, у свою чергу, – це образ без схожості. За визначенням філософа, у віртуальній реальності особа в її радикально штучно створеній версії здається копією без оригіналу, симулякром (нереферентною копією особи, яка відправляє до гіперреальності) [473, с. 267].

Симулякри є сконструйованим звабливим символічним за своїм характером об'єктом, орієнтованим на задоволення бажань споживача. Є неправдивою подібністю, умовним позначенням, що функціонує в суспільстві як його заступник. Як наслідок, сучасність є епохою загальної симуляції, яка створює гіперреальність і охоплює усі сфери життя особи, яка в епоху постмодернізму може не відрізняти справжнє від вигаданого. Реальність завершується, а її місце заміщує симулятивна гіперреальність симулякрів [318, с. 121].

Симуляція в інтерпретації Ж. Бодрійяра означає набуття символами, знаками, образами самодостатньої реальності. На його погляд, розвиток цивілізації наразі рухається в напрямку затвердження світу симуляцій, які поширились майже на всі сфери суспільного життя. Незалежно від побажань людини, різноманітні симулякри вже стали частиною сучасної буденності. Вони стають невіддільними від нових культурних продуктів, роблячи їх якісно невизначеними. Так, сучасна звукозаписувальна апаратура дозволяє проводити різноманітні маніпуляції зі звуком. Класичні твори Моцарта, Бетховена можуть набувати зовсім іншого, за різними параметрами, звучання, яке, тим не менш, може подобатися публіці. Більше того, сучасна апаратура дозволяє слухачам ставати співавторами виконання, задаючи звучанню певні якісні характеристики, водночас цей варіант виконання буде відрізнятися від варіанта, який був задуманий авторами твору. Це буде «копія копії» [262, с. 9].

Явище віртуальної особи не є настільки новим, як стверджують окремі дослідники, та певною мірою вже декілька тисячоліть проявляється в мистецтві,

а саме: в театрі, кіно та літературі. А такі художники як, Е. Уорхол, К. Ольденбург, Р. Раушенберг, Р. Ліхтенштейн та інші, більшість з яких були медійними особами, у своїй діяльності та презентації створювали симулякри самих себе – в картинах, поведінці, медійному просторі тощо.

Ще одна метафора, яка використовувалася Ж. Дельозом та Ф. Гваттарі – «тіло без органів», як віртуальний вимір людини. «Тіло без органів» – не виробляє, не споживає, служить поверхнею для реєстрації всього процесу виробництва бажань, що набуває актуальності в умовах культури споживання[472, с. 245]. У подальшому метафору «тіло без органів» інтерпретували послідовники Ж. Дельоза та Ф. Гваттарі. Так, у роботі «Дельоз та Інтернет», Я. Бюканан розширює концепцію «тіло без органів», стверджує, що кредитна картка, номер соціального страхування та інші персональні дані ладні надати досить багато інформації про життя, вподобання та звички особи. Можна припустити, що саме тому в інтернеті «плоть та кров» замінюється безтілесним цифровим «профілем» [352]. Можна стверджувати, що безкровний цифровий акаунт із персональними даними витісняє людину як біологічну істоту та стає все більш визначальним для її представлення в мережі «Інтернет», а ніж власне фізичні ознаки людини. Використовуючи метафору Я. Бюканана, цифровий акаунт стає тим самим «тілом без органів», що стає проєкцією людини в мережі.

З огляду на те, що під терміном «цифровий профіль або акаунт» (детально буде розглянуто у Підрозділі 2.1. «Концептуальні підходи до визначення права на цифрову ідентичність у мережі «Інтернет») розуміються не лише персональні дані, візуальні образи, а й вся інформація, яка генерується про особу та результати профілювання, за включенням псевдоанонімізованих даних, то метафора Ж. Дельоза та Ф. Гваттарі про зміст безкровних цифрових профайлів або «тіло без органів», якими є тілесність, свята, домашні тварини, фізична активність, сюжети візуальної комунікації, наповнюється сенсом.

Ж. Бодріяр у «Симулякрах та симуляції» пише про протез-двійник, який неодмінно знищує оригінал. Віртуальна реальність та спілкування в мережі

довгий час сприймалося науковцями як штучний замінник, наразі, нерозривно пов'язаний із повсякденним буттям.

Наступним викликом постає посилення сингулярності та проблема того, чи залишиться людина в існуючому вигляді Homo Sapiens або ризикує трансформуватися у природу транслюдської, постлюдської, генетично-модифіковної людини Homo Supertechnologicus, яка має виникнути в результаті використання гуманотехнологій [55, с. 32]. Футурологи застерігають про ризики порушення приватності внаслідок трансгуманістичної трансформації людства та створення, так би мовити, «нової людини», яка передбачає поєднання власного фізичного тіла з електронними пристроями, покликаними розширити когнітивні та творчі здібності людини.

Ідея запису персональних даних людини на електронних носіях, розміщених у тілі, що змінює біологічну сутність людини, із далекого майбутнього перетворюється в цілком фізичну реальність [109]. Крім того, відомі прогнози Р. Курцвейла про поширення застосування до 2030 року нанотехнологій або нанороботів, здатних потрапляти у кров людини для діагностування, лікування та покращення когнітивних здібностей [608, с. 187].

Технологічні трансформації вказують на гібридизацію людського та постлюдського в розвитку технологій. На відміну від минулих етапів розвитку суспільства, обумовлених розвитком технологій, на сучасному етапі удосконалення інформаційно-комунікаційних технологій може статися, що техніка, вийшовши із-під контролю, не буде служити інтересам людини, а людина ризикує стати частиною техніки. Так у сфері управління поступово проявляється тенденція передачі повноважень із прийняття юридично значущих рішень від людини до автоматизованих систем прийняття рішень.

Віртуалізація реального світу, як наслідок цифровізації, від вигадок та передбачень футурологів стає частиною повсякденного буття. Проєкти віртуалізації людського тіла [277, с.16], розвитку штучного інтелекту, IoT та системи Smart city, які об'єднують людей із навколишніми речами, технологічними пристроями, створюючи копії об'єктів фізичного світу у

віртуальному середовищі поступово стають частиною фізичної реальності. Відбувається певне поєднання, симбіоз людського та артефактного, коли суб'єкт задля адаптації має бути «вбудований» в існуюче технологічне середовище.

Цифрові комунікації стирають кордони між фізичним та цифровим, локальним та глобальним світами, що серед іншого спонукає до переосмислення сутності основоположних правових категорій, серед яких громадянство. У мережі втрачається значення державних кордонів, людина, стає громадянином глобального інформаційного світу, членом мережевої спільноти, що надає йому певні права та накладає обов'язки. М. Хаубен запропонував для позначення громадянства в мережі термін «Netizen», під яким розуміється віртуальний громадянин, користувач Інтернету [552, с. 35]. Надалі ідеї віртуального (мережевого) громадянина Netizen були відображені в роботах Р. Гальперіна та Дж. Бекхау [551, с. 43]. К. Моссбергер, запропонував схожу за змістом концепцію цифрового громадянства, під якою розуміється здатність особи брати участь у суспільному житті онлайн [676, с. 15]. Категорія цифрове громадянство також використовується в контексті технології цифрового акаунту особи та законодавчих ініціатив низки держав, направлених на набуття іноземцями громадянства онлайн. Х. Дженкінс, С.Л. Гам'єр-Томсон, Н. Клінгер-Віленчик та А. Ціммерман пропонують застосування концепції цифрового громадянства як конструкту людини у віртуальному середовищі [583, с.1482].

Серед наслідків цифрових трансформацій виокремлюється: глобальне транснаціональне громадянство або космополітичне (кібергромадянство) громадянство, яке завдяки цифровим технологіям дозволяє людям відчути себе часткою глобального співтовариства, де національні кордони держав втрачають значення, що дає відчуття спільної участі та відповідальності перед глобальними викликами; кібергромадянства для користувачів соціальних мереж як середовища для вираження громадянської позиції, здійснення права на об'єднання та свободу вираження; набуття цифрового підданства, яке наділяє низкою прав, обов'язків та покладає відповідальність за вчинювані порушення;

формування політичних спільнот, заснованих на інтересах та цінностях, без прив'язки до географічних кордонів держав тощо.

Л. Оргад вважає, що в результаті зростання глобальної взаємопов'язаності між особами та необхідності покладення відповідальності, може актуалізуватися питання створення міжнародної юридичної особи та цифрової ідентичності як форми «глобального громадянства» [728, с. 353].

У соціології аналізом зв'язків між наукою, технологією і «соціальним» займається акторно-мережева теорія або ANT. Відповідно до ANT, технології та соціальний світ розглядаються як пов'язані в гетерогенну мережу (неоднорідну за своєю суттю), яка включає в себе об'єкти та людей – або акторів.

Саме завдяки розвитку технологій, соціальних мереж, IoT, автономних систем, мови програмування, ідеї акторно-мережевої теорії, розроблені Б. Латуром та його послідовників, висловлені у 1990 роках, набули нового змісту. Науковці запропонували не проводити відмінність між людьми та речами (об'єктами) у здійсненні дії, прирівнявши людських та нелюдських акторів, матеріальні об'єкти та нематеріальні істоти, якщо вони займають позицію підмета. Акторно-мережева теорія об'єднує речі у світ людських дій та наділяє об'єкти здатністю впливати на результат дій Акторно-мережева теорія не використовує такі антропоцентричні терміни як «суб'єкт», «індивід», «особа», «агент», запозичивши із семіотики А.Ж. Греймаса нейтральну категорію як «актант». Під терміном «актант» розуміється хтось хто виконує певну дію або здійснює вплив: люди, речі, події тощо [4, с. 224]. Відповідно до ANT технології можуть стати частиною суспільства та впливати на людей.

Відповідно до ANT, актантом може виступати не лише людина, а й будь-яка діюча особа, сукупність осіб, об'єкт та подія, яка впливає. Наприклад, судження науковців у лабораторії, вплив мікробів та вірусів, виступ публічного діяча, запізнення публічного транспорту тощо [446]. Всі вони створюють різні конфігурації аналогічних вчинків. Таким чином, актанти набувають значення завдяки своєму місцю, взаємодії та впливу один на одного. Наприклад, працівник на роботі є складовим елементом акторної мережі, в яку входять його

співробітники, офіс, комп'ютер, стілець, стіл тощо. Такі об'єкти можуть вчиняти дії по відношенню до особи або бездіяти. Усі актанти, як-то артефакти, тварини, машини опиняються на єдиному онтологічному рівні. Для набуття більшого впливу в мережі, актантам необхідно взаємодіяти та об'єднуватись у союзи. Б. Латур дотримується принципу, що будь-які актори повинні розглядатись як рівноправні актори (актанти), пов'язані разом у мережі, об'єднані для досягнення певної мети. Отже, актором (актантом) мережі може виступати автоматизована система (ШІ), цифрова репутація, система IoT, що здатна впливати на людину та її можливість здійснення прав та обов'язків у фізичному та цифровому світі.

Атоми та молекули є такими ж діючими особами як банк, фінансова установа або Олімпійські ігри 1976 року. За твердженням дослідників, що в межах акторно-мережевої теорії потенційно агентністю володіє будь-який об'єкт, здатний брати участь у дії, не відрізняючись від людей, тварин, технічних засобів та будь-яких інших акторів – не людиною. У такому розумінні агентністю володіє будь-який об'єкт, здатний впливати та вносити будь-які зміни у фізичне середовище. За твердженням Б. Латура, дія є там, де відбуваються зміни, а якщо зміни не відбуваються, то немає дії [620, с. 170].

Перевагою ANT є розгляд суспільства як гетерогенної мережі, під якою розуміється результат складно взаємопов'язаних мереж людей, організацій, агентів та машин [621, с. 379].

Означене дійсно відображає певною мірою ситуацію, яка відбувається в інтернеті та соціальних мережах, де найвагоміший вплив, популярність, найвищі продажі товарів та послуг має користувач – блогер, із найбільшою кількістю підписників та переконливою цифровою репутацією. До того ж, за цифровим профайлом успішного блогера може стояти не лише фізична та юридична особа, а й нейронна мережа, візуальний та контекстуальний контент якої подекуди складно відмежувати від особи з фізичного світу [118; 258].

Крім того, мережевий вплив та застосування ANT можна простежити у взаємодії між людиною та ШІ, взаємодії, яка виникає в системі охорони здоров'я внаслідок впровадження новітніх технологій. Утворюється єдина мережа, яка

охоплює не лише автоматизовані системи в галузі медицини, але й користувачів, медичних працівників та інші технології. ANT пояснює, як виникають мережеві взаємодії та відносини, коли автоматизовані машини будучи частиною мережі (об'єднання) людей, володіють здатністю діяти як актори.

Слід визнати, що застосування теорії, яка наділяє матеріальні об'єкти статусом рівним із людьми у виробництві дії як активних агентів, ставить виклик не лише соціології [620, с. 369]. Дискусія щодо правового статусу автономних інтелектуальних агентів також відбувається в юриспруденції.

Хоча застосування ANT зазнає критики, в тому числі через нехтування правам людини, які залишаються за межам її розгляду. У розумінні Б. Латура, акторно-мережева теорія може бути застосована не лише як теорія пізнання, а як метод дослідження, описання та вивчення трансформації союзів, спільнот між гетерогенними актантами [618, с. 20; 619, с. 45].

Технологія одночасно формує суспільство і може розглядатися як інститут, вбудований у соціотехнічні мережі між людьми та об'єктами матеріального світу. У такій схемі користувачі технологій є зацікавленими сторонами.

Теорія мереж зарекомендувала себе як інструмент пізнання в різних дисциплінах, у тому числі в юриспруденції. Наприклад, крізь призму теорії мереж Д. Макгоун досліджує взаємопов'язаності та вплив інтелектуальної власності та антимонопольного законодавства [663, с. 514]; Л. Страгілевиць аналізує порушення права на недоторканність приватного життя, оскільки поширювана про особу інформація в мережі може бути публічного чи приватного характеру [802, с. 919]; М. Лаві аналізує відповідальність постачальників [622, с. 855]; М. Дженнеджон, Л. Бернштейн, А. Шварц досліджують проблеми договірного права [584, с. 71; 331, с. 1009; 784, с. 325]; А. Ліор аналізує деліктну відповідальність у разі шкоди, заподіяної ШІ [641, с. 12] тощо.

А. Ліор зазначає, що теорія мереж описує окремі об'єкти, «вузли»; якщо в мережі бере участь автоматизована система, вузлом буде штучний інтелект (алгоритм), зокрема відносини та вчинки, що об'єднують «вузли»,

називатимуться ребрами [641, с.14]. Ці чинники являють загальний погляд на світ або систему як на нескінченну кількість ребер (підстави виникнення відносин), які об'єднують різноманітні «вузли» або акторів. Такий погляд дозволяє проаналізувати пов'язані системи з різних точок зору, використовуючи різні вимірювальні властивості. За твердженням науковця, характеристикою мережі може бути її «обмеженість», яка проявляється в окресленні її кордонів. Визначення кордонів мережі може бути суб'єктивним та залежати від точки зору спостерігача. Науковець наводить приклад деліктних правовідносин, де притягнення до відповідальності за шкоду, завдану автоматизованою системою буде здійснювати уповноважений орган. Науковець пропонує розглядати мережу цивільно-правових відносин як обмежену вузлами або кордонами, що визначаються нормативно-правовими актами, дотримання яких забезпечується органами, в тому числі може обмежуватися самою автоматизованою системою або програмним кодом, який окреслює межі допустимої поведінки в системі – мережі. Науковець зазначає, що в мережі набуває значення: ступінь пов'язаності вузлів, структурованість мережі (централізована, децентралізована або розподілена), стабільність або динамічність, значення або вплив мережі.

Пов'язаність вузла або – відстань, яка пов'язує вузли або мінімальна кількість кроків, які пов'язують акторів. Так, значущість та характер зв'язків (шлюб, партнерство, дружні або трудові відносини тощо) може опосередковано свідчити про їх міцність, централізованість тощо. Характер зв'язку може надати інформацію, зокрема про те, як швидко нова подія (наприклад, у вигляді інформації) може поширюватися по всій системі. Ступінь та характер пов'язаності вузлів або акторів впливає на структурованість мережі.

Під структурованістю мережі А. Ліор пропонує розуміти комбінацію вузлів та ребер у системі, що визначає «вагу» або «значущість вузла». Структура мережі залежить від того, як були сформовані відносини між вузлами. Структура мережі може бути децентралізованою або розподіленою. Розподільна система відноситься до мережі, в якій зв'язки між вузлами генеруються випадковим шляхом, що призводить до відносно рівномірного розподілу його меж. У такій

системі значущість будь-якого вузла розподілена по всій системі, а розміщення вузлів відбувається зрідка, в порівнянні з централізованою мережею. Децентралізована мережа переважно породжується локальними середовищами [641, с. 30].

Як визначає А. Барат у цьому контексті, що значущість вузла, буде визначатися вагою ребер, які їх з'єднують [328, с. 3747]. Це засновується на твердженні, що не всі «ребра» мають однакову значущість (вплив). За визначення М. Грановетера, в соціальному контексті міцність відносин у соціальній мережі можна розглядати як тривалість, емоційну інтенсивність або близькість [543, с. 1360]. Ці властивості допомагають визначити значущість або «вагу» ребра, під якою також розуміються підстави виникнення відносин. У разі завдання шкоди автоматизованою системою ШІ, мережу будуть складати «вузли» (система ШІ, особа, якій завдано шкоду, принципал, розробники системи та ін.) та «ребра», які їх пов'язують (характер та підстави відносини. Наприклад, функціонування автоматизованих алгоритмів, які збирають персональні дані, в результаті їх аналізу формують рейтинг та цифрову репутацію суб'єкта в мережі. Характер, інтенсивність взаємодії фізичної особи (проведення публічної діяльності, публікацій тощо) із іншими користувачами, участь та активність на різноманітних платформах, сервісах визначають вагу такого учасника та його рейтинг у мережі (цифрову репутацію), вплив на інших користувачів та можливість отримання доходів від діяльності в мережі прямо або опосередковано [640; 641, с. 20].

Враховуючи зазначене, що погляд на відносини крізь призму мережевих зв'язків має значення в дослідженні відносин завдання шкоди програмним інтелектуальним агентом, оскільки дозволяє побачити, як за автоматизованою програмою завжди «ховається» фізична особа. Теорія мереж надає додаткові інструменти пізнання суспільства та права, дозволяє врахувати вплив новітніх технологій на сучасні правовідносини.

Окрім гетерогенності відносин у мережі «Інтернет», доцільно також завернути увагу на такий їх характер, як транскордонний. Цифрове середовище

є вільним від територіальних кордонів держав у традиційному розумінні та характеризується транскордонним характером, що впливає на особливості формування правовідносин у мережі. Водночас на структуру мережі впливає існування вільного та ізольованого інтернету КНР. Користувачі, крім традиційної приналежності певній національній державі із відповідними правами та обов'язками, завдяки глобальному та транскордонному інформаційному середовищу, набувають властивості приналежності глобальному середовищу.

Враховуючи викладене, статус фізичної особи, можливість здійснення права та обов'язків у мережі породжуються не лише наявністю тих чи інших правових норм, а й таких не юридичних факторів як: існування цифрових технологій, інших користувачів та сервісів, цифрового середовища, яке детермінує, які саме права та обов'язки існуватимуть у фізичної особи в мережі. У результаті на здійснення правосуб'єктності фізичної особи у фізичному світі впливають такі не юридичні фактори, обумовлені розвитком інформаційних технологій, як: доступ до мережі, функціонування автоматизованих алгоритмів; взаємодія з платформами та користувачами, соціальні зв'язки та виникаючі взаємозалежності між користувачами; коментарі та відгуки (позитивні або негативні), лайки, завантажені фото та відео інших користувачів, які здатні підіймати (опускати) рейтинг та формувати цифрову репутацію в мережі «Інтернет»; збір та обробка персональних даних автоматизованими система та IoT; взаємодія із інтелектуальними агентами тощо. У мережі фізична особа майже опиняється на єдиній площині із алгоритмами, інтелектуальним агентами, які значно впливають на її можливість здійснення прав та обов'язків у фізичному світі.

За твердженням низки науковців, цифрова ідентичність є основою для нової ери взаємодії між урядом та громадянами, надає доступ до інформації та послуг, забезпечує цілісність цієї ідентичності, набуває все більшого значення. К. Саліван прогнозує, що цифрова ідентичність незабаром стане основним засобом доступу до державних послуг, оскільки більшість їх буде надаватися

виключно в цифровому просторі. Досліджуючи цифрові трансформації в Австралії, науковець стверджує, що цифрова ідентичність використовується для доступу до державних послуг у сфері охорони здоров'я, оподаткування, судочинства та впровадження режиму «без паперу». У зв'язку із збереженням можливості надавати паперові документи до державних установ, створюється хибне враження про можливість вчиняти правочини поза цифровою системою, водночас всі паперові форми документів обробляються та вносяться до електронних реєстрів та цифрових систем [805].

Підтвердженням вищезгаданої тези є масова цифровізація, розвиток електронного урядування [491], електронних державних земельних кадастрів, електронного судочинства [39, с. 447], [40] в різних куточках світу [37, с. 185], [41, с. 5], [42, с. 285], [38, с. 759], автоматизації виконавчого провадження та альтеративного вирішення спорів [63, с. 200], запровадження Системи Європейської цифрової ідентичності, яка передбачає об'єднання у єдиному додатку національні цифрові посвідчення особи для транскордонної ідентифікації та автентифікації [440; 343].

Україна також не стоїть осторонь цифрових трансформацій. Поступово запроваджуються послуги електронного уряду, електронного судочинства, впровадження режиму «без паперу» та цифрової ідентичності, розширюється коло послуг, які надаються дистанційно та із застосуванням додатку «Дія» [235, с.86; 275]. Також зростає кількість документів, доступних у застосунку «Дія» [250]. Введення воєнного стану та поширення COVID-19 прискорили процес цифровізації в України [24].

Наразі не лише цифрові акаунти в різноманітних державних системах є необхідною умовою оперативного доступу до держаних та комунальних послуг, а й акаунти у соціальних мережах, які представляють автентичну фізичну особу в мережі «Інтернет», є запорукою довіри та репутації для подання заявок на стипендії, гранти, навчальні програми та навіть подання документів на візу США. А відсутність сторінки в соціальній мережі ставить під сумнів довіру до особи. Цифрова ідентичність у мережі «Інтернет», яка представляє автентичну

фізичну особу, стає необхідною передумовою ефективного здійснення прав та обов'язків у фізичному світі.

Вищезазначене трансформує уявлення про фізичну особу як суб'єкта цивільних відносин у мережі «Інтернет». Природні властивості людини до комунікації наділяють її статусом особи. Єдність структури особистості утворюють свідомість, воля, здатність до творчості тощо. У свою чергу, в цифровому середовищі на перший план виходить сутність людини не як біологічної істоти, а як здатність побудови зав'язків, комунікації, здійснення впливу своїми діями на інших учасників комунікації та відносини.

Вищевикладене дає підстави стверджувати, що на здійснення прав та обов'язків фізичної особи як у фізичному, так і у віртуальному світі впливають дії, вчинені в мережі «Інтернет»: алгоритми обробки даних, які приймають індивідуалізовані рішення відносно суб'єкта; персональні дані, які розкрили треті особи (вірусні відео, створення фотомемів, неактуальні та застарілі публікації про особу (дали поштовх для започаткування права на видалення) тощо. У свою чергу, в мережі «Інтернет» фізична особа є представленою цифровою ідентичністю – системою даних, які являють цифрову ідентичність.

Викладене дозволяє стверджувати, що в науці розробляються досить різноманітні підході до розуміння та переосмислення особи під впливом інформаційних технологій, які заслуговують уважного аналізу та можуть бути враховані при проведенні подальших досліджень. Цифрові трансформації неминуче розширюють можливості здійснення прав у мережі, поряд з цим стикаються з викликами. Поступове занурення в цифрове середовище здатне посилювати нерівність між людиною та технологіями, де людина ризикує програти нейронним мережам та отримати статус неконкурентоздатної. Слідування позиції, що в цифровому середовищі на перший план виходить цифрова ідентичність – система даних фізичної особи в інтернеті, покликано допомогти дослідити специфіку виникнення та припинення правоздатності в мережі, виникаючі нові цифрові права, новітні засоби ідентифікації в мережі, запровадження єдиної цифрової ідентичності на платформі блокчейн, втручання

в недоторканність приватного життя в мережі та проблему захисту персональних даних, існування яких опосередковується технологіями. Застосування такого підходу дозволяє прослідкувати, як із поступовим делегуванням прийняття незначних дій (підбір квитків, вибір маршрутів для подорожей, сплата автоматичних платежів), фізична особа передає автоматизованим система вчинення все більшої кількості юридично значущих дій, які несуть доленосні наслідки (фінанси, інвестування, працевлаштування, урядування, збройні конфлікти тощо). Можна спостерігати, як коло дій, які делегуються, від початку здаються рутинними та малозначущими, поступово розширюються до юридично значущих. Тому по мірі такого делегування зростають ризики для здійснення прав та фундаментальних свобод людини. Вкрай важливо забезпечити контроль за алгоритмами та не допустити ситуацію, при якій рішення про позбавлення людини життя буде приймати автоматизована система. Така ситуація потребує розробки юридичних гарантій та технологічних засобів залишення контролю за функціонуванням систем саме за людиною.

1.2. Мережа як чинник трансформації юридичної природи фізичної особи

Знаходячись на початку четвертої промислової революції, яка докорінно змінює спосіб життя, поширює застосування роботизованої техніки та ставить виклики, які за масштабами своєї складності не схожі на те, що людство переживало досі. Революція несе безмежні можливості підключення мільярдів людей за допомогою мобільних пристроїв, що створює безпрецедентну потужність обробки, зберігання даних і доступ до знань. Технологічний прорив, що охоплює різноманітні галузі, такі як штучний інтелект, робототехніка, IoT, автономні транспортні засоби, 3D-друк, нанотехнології, біотехнології та квантові обчислення тощо. Багато з цих інновацій ще розробляються, але вони здатні підсилювати один одного [782].

Відбуваються глибокі зрушення в усіх галузях, що відзначаються появою нових бізнес-моделей – підривних інновацій, втратою лідерства успішними компаніями та зміною систем виробництва, споживання, транспортування доставки тощо. Змінюється парадигма у способах роботи, спілкування, вираження, надання державних послуг, отримання освіти, охорони здоров’я тощо [430, с. 44].

Як зазначає письменник А. Грінфілд, технології в тому чи іншому вигляді (камери зовнішнього спостереження, нейронні мережі, автоматизовані алгоритми, що регулюють повсякденність та оцифровують буденність) опосередковують щоденні вчинки людини, змінюючи навколишнє суспільство. Без смартфона сучасна людина вже не уявляє своє існування в новій цифровій реальності. Смартфон став щоденною необхідністю, якому довіряють та передоручають дедалі більше функцій. Суспільство відкрито виражає готовність обміняти недоторканність приватного життя на зручність, приймаючи соціальний договір, умови якого подекуди залишаються невідомими. Смартфон стає, так би мовити, «протезом», а в його владі перебуває значний соціальний простір, який дозволяє опинитися в різних місяцях, але водночас у жодному не

бути присутніми повністю, фізична особа перетворюється в мережевого індивіда, нового суб'єкта у зміненому світі [755, с. 50].

Сучасне суспільство характеризується високим рівнем взаємопов'язаності та взаємозалежності, а ніж будь-коли [439, с. 7]. Технології та інфраструктури мережі стали невід'ємною частиною сучасного життя. Так, сучасні міста не можуть функціонувати без мережевих технологій утилізації відходів, каналізації, електромереж, водопроводів, транспорту, розподілу товарів, продуктів харчування та послуг, охорони здоров'я, освіти, телекомунікацій, банківських та адміністративних послуг. Більшість цих мереж поширюються на регіональному та глобальному рівнях, створюючи мережі мереж, які утворюють «павутину людства» [861].

У 1929 році угорський письменник Ф. Карінті у фантастичному оповіданні «Мережеві зв'язки» висунув твердження про взаємозв'язок між головними героєм оповідання та його друзями з будь-якою людиною на землі через п'ять інших людей. Автор припустив, що будь-яку людину у світі розділяють не більше п'яти знайомих та друзів [687, с. 77].

«Проблема малого світу» захоплює науковців у різних сферах знань. Наприклад, класична модель мережі, яка відома як випадковий граф, була вперше описана математиком і біологом А. Рапопортом на початку 1950-х років, а згодом наново відкрита та проаналізована П. Ердо та А. Рені [504, с. 17].

У 1950-х роках соціолог та математик І. де Сола Пул та М. Кохен, провели дослідження, присвячене соціальним зв'язкам та математично довели висунуті твердження щодо «ефекту малого світу» [687].

У 1967 році психолог С. Мілгрем довів у власному дослідженні проблеми «малого світу», гіпотезу, що ланцюжок лише в п'ять осіб здатний зв'язати двох різних людей на планеті. Експеримент С. Мілгрема був обумовлений бажанням зрозуміти пов'язаність людей між собою та з'ясувати ступінь пов'язаності між двома випадковими особами у США, відповівши на питання, скільки знайомих осіб необхідно, щоб їх з'єднати. Науковцю вдалося довести, що світ являє

набагато меншу соціальну мережу взаємопов'язаних осіб, ніж це може здаватися [835, с. 425].

Facebook провів власний експеримент, заснований на ідеї С. Мілгрема, який підтвердив зростаючу взаємопов'язаність між користувачами в різних куточках світу. За результатами дослідження, у 2016 році, коли активними користувачами Facebook було 1,5 млрд осіб, двох випадкових користувачів Facebook у різних куточках планети розділяли лише три з половиною людини [496]. Проведений експеримент дозволив довести, що сучасне суспільство являє тісно пов'язану мережу.

Поряд із тим, відповідно до теорії «слабких зв'язків», висунутої М. Грановеттером у 1973 році, істотний вплив на людей та їхнє життя, можливість досягнення цілей здійснює підтримання комунікації з близьким оточенням (рідні, друзі, сусіди). Поєднання «сильних і слабких» зв'язків сприяє зниженню роз'єднаності людей. «Слабкі», довільні зв'язки об'єднують відокремлені спільноти або «скупчення людей». За твердженням науковця, така структура мереж та взаємопов'язаність населення в масштабах планети в майбутньому стане однією з причин стрімкого поширення хвороб, чуток, інформації та нових технологій [543, с. 1360]. Стрімке поширення Covid-19, інформаційні війни, коливання фінансових ринків підтверджують висунуту тезу науковця. Інтернет змінює уявлення про «близькість» та «віддаленість», оскільки особа виявляється близькою до людей, географічно віддалених від неї, впливає на них та стимулює зростання довіри до людей, «лідерів думок», які формують нові тренди, цінності, поширюють ідеї, з якими користувачі особисто не знайомі.

Наразі соціальні платформи не лише використовують вже існуючі мережі взаємозв'язків між людьми, а й посилюють їх. З урахуванням того, що технологічний прогрес робить дедалі очевиднішою значущість мереж у повсякденному житті людства, значення мереж не можна недооцінювати. Наразі для здійснення впливу на великі маси людей, навіть державні органи влади, політичні діячі звертаються до новітніх інструментів та соціальних мереж.

Термін «мережа» як така використовується для позначення структурних утворень у різних дисциплінах. Дж. М. Подольні та К. Л. Пейдж використовують категорію «мережева форма організації», під якою розуміють будь-яку сукупність акторів, які підтримують постійні, тривалі відносини обміну один з одним і, в той же час, не мають легітимної організаційної влади для вирішення спорів, які можуть виникнути під час обміну [742, с. 57]. За визначенням М. Калера, термін «мережа» протиставляється таким альтернативним структурам як ринок та ієрархії [590]. Дедалі більше визнається роль мереж та розвиток «теорії систем» у таких галузях як: біологія, інженерія, інформатика, управління тощо [671, с. 533].

Серед спільних характеристик мережі називається: спільна участь, процес, дотримання, правозастосування та інституціоналізація [688, с. 244]. Термін «мережа» в різних дисциплінах відображає групу неієрархічних, водночас взаємозалежних суб'єктів [623, с. 246]. Такі суб'єкти демонструють високий рівень неформальної співпраці. Завдяки властивостям мережі, мережева структуризація пропонується як альтернатива традиційній організації та нормотворчості, що може забезпечити оперативне та ефективне реагування перед виникаючими викликами. З одного боку, ієрархії являють собою організаційну модель, в основі якої лежать правила, що визначають структуру і напрям діяльності [825]. З іншого боку, ринки значною мірою децентралізовані і досягають координації за допомогою інтуїтивних методів, таких як надання сигналів [794]. Мережі не є жорсткими як ієрархії, та не є гнучкими (динамічними) як ринки. Навпаки, мережі містять більше неформальних зв'язків, ніж жорстко бюрократизовані ієрархії, при цьому характеризуються складнішою організаційною координацією, яка виходить за межі звичних сигнальних механізмів ринків. Р. Холтон зазначає, що мережі виникають саме там, де ринки та ієрархії відсутні або не можуть забезпечити необхідну чи оптимальну організаційну платформу для взаємодії [562, с. 170].

Достеменно не встановлені чинники, які спонукають виникнення мереж. На погляд Р. Холтона, мережа як організаційна структура може виникати та

зберігатися протягом певного часу, через зручність або по інерції. Якщо ієрархічна структура характеризується підпорядкованістю, структурованістю та бюрократичністю, відсутністю гнучкості та оперативності, то особливістю ринкової організації може бути короткотривалість, яка може не забезпечувати учасників досягненням бажаних результатів [562, с. 170]. У свою чергу, мережа, будучи гібридною організаційною формою, характеризується гнучкістю, що притаманна ринкам, та структурністю, яка властива ієрархічній структурі. Так, у мережі існує певний розподіл влади, ієрархія та управління [425, с. 122]. Р Холтон зазначає, що мережі реагують на виклики досить оперативно в порівнянні з ієрархічними структурами, і більш ефективно в порівнянні з ринковими організаціями. Означені три організаційні моделі можуть співіснувати.

За твердженням Е. Лаумана, з точки зору структури, трихотомія між ринковою, ієрархічною та мережевою формами організації є хибною. Ринки та ієрархії є двома типам організації, які можна представити за допомогою базових мережевих аналітичних конструкцій вузлів та зв'язків. Науковець наводить приклад фінансового ринку, як обмеженого майданчика осіб, де кожний учасник ринку представлений «вузлом», який не має зв'язків з іншими учасниками – «вузлами». У свою чергу, ієрархія розглядається з точки зору централізованої мережі, в якій переважна більшість зв'язків спрямовується до одного конкретного суб'єкта – «вузла» або від нього. З точки зору структури, кожна форма організації є мережею, а ринок та ієрархія є лише проявами більш широкого типу [612, с. 90].

Можна зазначити, що в окремих системах мережева структура є очевидною відразу, як наприклад, мережа «Інтернет» та соціальні взаємозв'язки в суспільстві, рух хімічних часток та поширення хвороб, розподіл продукції, взаємодії між органами державної влади. Це обумовлює інтерес дослідників звертатися до мережевого методу для дослідження. Розгляд суспільства крізь призму мереж, екстраполяція мережевого методу на різні сфери наукових досліджень характеризується істотними перевагами та значущістю.

За твердженням К. Раустіала, такі галузі як екологічне право, міжнародні економічні відносини дедалі частіше стикаються з викликами, які вимагають нового типу міжнародної координації, які можуть бути вирішенні в разі застування мережевого підходу співробітництва таких міжнародних установ як: ООН, Міжнародний валютний фонд, Всесвітня організація охорони здоров'я та ін. Науковець стверджує, що мережева модель співробітництва держав та міжнародних організацій завдяки неформальності, гнучкості має сприяти її учасникам у забезпеченні рівних можливостей міжнародного співробітництва для досягнення спільно поставленої мети [762, с. 205].

Для глибинного розуміння мереж фахівці у різних наукових галузях розробляють інструменти (математичні, статистичні тощо), які дозволяють глибинно дослідити мережеві відносини.

На думку Я. Парвіайнена та М. Кекельберга, створений у 2017 році людиноподібний робот «Софія» відіграє певну політичну роль у формуванні середовища комунікації зацікавлених осіб. У процесі обміну знаннями відбувається залучення нових учасників у мережу акторів [734, с. 715].

Крім того, застосування соціальних теорій у праві покликане допомогти взяти до уваги пов'язані з цим інтереси учасників суспільних відносин для цілей удосконалення правового регулювання.

Слід зазначити, що застосування теорії мереж до політичних та правових досліджень проводились, у тому числі, до розроблення акторно-мережевої теорії. Застосування концепції мережі по відношенню до державних та недержавних акторів, вперше були застосовані науковцями у 1950-1960-х роках, проте ці напрацювання не отримали достатньої підтримки в юриспруденції [688, с. 245].

Н. Бантека досліджує застосування мережевого підходу в галузі міжнародних відносин, співпраці в розробці міжнародно-правових норм, що дозволяє поглибити розуміння міжнародного співробітництва. Відповідно до мережевого підходу, науковець застосовує терміни «вузли» та «актори» по відношенню до учасників міжнародних відносин. Науковець не розмежовує акторів, які можуть бути учасниками мережі, включаючи до їх числа держави,

міжнародні організації, неурядові організації, міжнародні чи національні судові органи, трибунали, корпорації та приватних осіб тощо. Науковець обґрунтовує тезу, що вирішальним чинником ефективної участі у відносинах є тісний взаємозв'язок та співпраця між учасниками нормотворчих міжнародних процесів [323, с. 350].

Розгляд міжнародних відносин крізь призму мережі, на думку Н. Бантекі, дозволяє визначити найвпливовіших акторів-лідерів, оцінити їх вплив на розвиток правотворчості в мережах, ефективність співпраці та взаємодії, доводячи зростаючий вплив та значення взаємозв'язків між державними та недержавними акторами у створенні міжнародних правових норм в інтернеті. Застосування мережевого підходу може бути цінним у співробітництві міжнародних організацій та установ, у розробці підходів для подолання викликів цифрової нерівності між державами, нерівності, обумовленої автоматизацією процесів та виникненням ізольованих цифрових середовищ внаслідок різних підходів держав до правового регулювання інтернету. Таким чином, здатність коригувати розумові лінзи та розглядати суспільство крізь мережу, надає науковцям додатковий набір методів та допомагає розробити пропозиції для удосконалення правового регулювання відносин у мережі «Інтернет». З огляду на всеохоплююче павутиння взаємозв'язків між фізичними особами, організаціями та подіями, привертає інтерес розгляд громадянського суспільства крізь «лінзи» мережевої структури, простежити взаємозв'язки, що виникають, і чинники, що впливають на його учасників.

Підтвердженням вищезгаданої тези є твердження винахідника Всесвітньої мережі Т. Бернерса-Лі про те, що майбутнє інтернету за «семантичним павутинням», де всі елементі життя людини в онлайні нерозривно пов'язані. У семантичній мережі про місце вчинення правочину особі нагадує банківська квитанція, фотокартка в телефоні та відео з камер відеоспостереження із біометричною ідентифікації. Таке майбутнє пов'язане зі «створенням безшовної мережі всіх даних у житті людини», – за твердженням науковця [770].

Розвиток семантичної мережі можна спостерігати на прикладі розумних міст. Уперше у 2008 році Google використала форму семантичної мережі в місті Нанаймо в Канаді. Місцева влада надала Google інформацію про функціонування пожежних служб, графік вивезення сміття, місцезнаходження кладовищ та інші дані роботи комунальних підприємств, які були включені до мап Google Earth, дозволивши мешканцям спостерігати за функціонуванням підприємств: вивезенням сміття, місцезнаходженням служб надзвичайних ситуацій неподалік від будинку та ін.[339, с. 313]. Подібне агрегування інформації є одним із кроків на шляху створення семантичної мережі[507]. Автоматизована програма збирає, обробляє, аналізує та порівнює дані та документи, підриваючи засади недоторканності приватного життя.

Дана ідея підтримується, в тому числі, іншими фахівцями та науковцями. В інтерв'ю Financial Times, генеральний директор Google Е. Шмідт у 2007 році визнав, що метою компанії є організація повсякденного життя користувачів [366]. Віце-президент Google з інженерних питань У. Манбер підтвердив, що компанія прагне розуміти наміри користувачів та давати відповідь на їх питання [339, с. 336]. Слід констатувати, що в середині нульових, коли була висловлена ця точка зору, в Google Search дійсно не вистачало даних для передбачення майбутніх дій користувачів. Наразі не лише пошукові системи збирають та обробляють дані користувачів, а й технології IoT, всі пристрої, що мають доступ до мережі «Інтернет». Окулус, збирає та обробляє рухи голови, рук та очей, особливості вади [639]. Розробники програмного забезпечення збирають та обробляють дані щодо емоційних реакцій користувачів, обсяги споживання електроенергії, місцезнаходження, поведінку на дорозі, дані біосенсорів та дані уподобань приватного життя [876, с. 25]. Зазначені персональні дані не лише збираються, обробляються розробниками, можуть також передаватися третім особам з метою проведення досліджень. До того ж відповідно до результатів обробки дані користувачів можуть підлягти профілювання, а профілі користувачів оцінюватись відповідно до стану здоров'я, освіти та здібностей.

Розвиток розумних міст, розподілених реєстрів, IoT, цифрових грошей, віддаленої біометричної ідентифікації, цифровізації державних сервісів, документів та посвідчень особи в єдиному додатку несе не лише комфорт та зручність, а й має зворотню сторону. Результати дослідження, проведені Л. Флак, С. Хофманом свідчать, що розвиток інфраструктури розумного міста впливає на здійснення права на недоторканність приватного життя, свободи вираження думок не лише позитивно, а й негативно [515]. Оскільки використання таких технологій як GPS-стеження, відеоспостереження несе ризики втручання у права на недоторканність приватного життя. Як стверджують науковці, особи схильні до самоцензури, ухиляються від публічних висловлювань та вираження думки через побоювання переслідування, що обмежує свободу вираження їх думки та слова. Крім того, стримуючим фактором залишається цифровий розрив.

На думку М. Марсала-Лакуна, технології розумного міста нехтують людиноцентричним підходом та ігнорують потреби та права людини [652, с. 563]. Слід констатувати, що така ситуація відобразилася на критеріях, започаткованих в Індексі розумних міст у 2019 році та провідного принципу, що умовою включення до рейтингу має бути дотримання людиноцентричного підходу під час впровадження новітніх технологій у місті [578].

Специфіка сучасного світу характеризується множинністю параметрів, а елементи знаходиться між собою у складній взаємодії та взаємозалежності. Означене ускладнює можливість прогнозування майбутніх перспектив розвитку суспільства. У сучасному суспільстві, коли відбувається оцифрування всіх сфер суспільства, втрачається межа між віртуальним середовищем та реальним світом, відбувається їх взаємопроникнення.

Поширення інформаційно комунікаційних технологій, серед яких технології розумного міста, розвиток елементів мережевих структур, змінюють суспільство, характер та соціально-політичні відносини. Дані трансформації підштовхнули до розробки іспанським соціологом М. Кастельсом концепції мережевого суспільства, під яким розуміється громадянське суспільство, яке організовано за принципом мережі, відмінною ознакою якої є автономія окремих

її членів та неформальне лідерство, на відміну від традиційних соціальних структур заснованих на ієрархії [418, с. 238].

Учасниками цифрового суспільства можуть бути як фізичні особи, так і автоматизовані системи. Структура цифрового світу, за твердженням науковця, як «мережі» визначається програмою, яка ставить задачі та правила, складається з програмного коду, який містить оцінку та критерії успішного та неналежного виконання правил», а «встановлена та запрограмована мережа дотримується інструкцій та правил, занесених до операційної системи, та здатна до самостійного формування в межах параметрів, заданих задачею та методами» [418, с. 239].

М. Кастельс вважає, що у світі мереж можливість здійснювати контроль визначають такі провідні механізми як: здатність створювати та програмувати діяльність мережі для досягнення поставлених задач; здатність об'єднувати та забезпечувати взаємодію різних мереж. У таких умовах програмування мереж стає формою реалізації влади у глобальному цифровому мережевому суспільстві цифрових громадян, де владний влив набувають ті, хто програмують та перепрограмують мережу[418, с. 240].

Поряд із категорією мережевого суспільства в науці висувається категорія «цифрового суспільства», під яким розуміється суспільство, яке створюється в результаті інтеграції інформаційно-комунікаційних технологій, будинків, офісів, навчальних закладів, використовує бездротове підключення, є залежним від функціонування цифрової економіки, підтримується цифровими інструментами, технологіями та залежить від інформаційних знань та цифрових продуктів [733, с. 2].

Таким чином, у світі, що бурхливо змінюється, вся соціально-економічна, політична структури поєднанні інформаційними каналами, які у сукупності з акторами складають мережу. За визначенням науковців, мережевій структурі поряд із взаємопов'язаністю властива децентралізація.

На формування концепції мережевого суспільства вплинули не лише ідеї М. Кастельса, Б. Латура та інших науковців, а й концепція глобалізації та ідеї

французьких філософів Ж. Дельоза та Ф. Гваттарі. Інформатизація, зокрема поширення інтернету називається технологічною передумовою глобалізації, як процесу становлення мережевого суспільства. Власне поширення інтернету та інформатизація виступають найістотнішими проявами поширення мереж. Поряд із цим, з позиції глобалізації взаємозв'язок цих явищ можна розглядати й у зворотному порядку. Тож характеристика сучасного суспільства як глобального, інформаційного та мережевого пов'язана між собою не випадково.

М. Кастельс стверджує, що процес глобалізації та зростання «комунальних ідентичностей» ставить виклик державам-націям, в умовах розширення сфери глобального управління. Цей підхід відображає соціологічну сутність цього явища. У юридичному сенсі використання мережі «Інтернет» є лише формою, можливістю здійснення будь-якого права, зокрема права на об'єднання [418, с. 240]. Глобалізація формує єдине геоекономічне середовище, яке опосередковане економічними, інформаційними, соціокультурними, комунікаційними, екологічними та іншими зв'язками, що перебувають у взаємозалежності.

Саме розвиток інформаційно-комунікаційних технологій, автоматизації та цифровізації, а з тим із оцифрування у всіх сферах людського буття стали поштовхом до глобалізації та ще більш очевидною мережевою структуризацією суспільства.

Одним із прикладів автоматизації та цифровізації є використання систем штучного інтелекту в роботі органів державної влади та місцевого самоврядування. У роботі податкових органів Франції використовуються аерофотокартки, зроблені Автоматизованою системою Національного інституту географічної та лісової інформації (IGN). Алгоритм дозволяє отримати контури будівель та басейнів із загальнодоступних аерофотокарток, з якими може ознайомитися на вебсайті. Автоматизована програма перевіряє правильність розрахунків та оподаткування місцевими податками (зокрема податком на нерухомість), шляхом порівняння даних, які містяться в поданих деклараціях, із об'єктами, виявленими на аерофотокартках. Агент податкової служби перевіряє

виявлені відхилення перед укладенням будь-якого правочину із нерухомістю [696].

Означена ситуація відображає, що поступово відбувається передача функцій соціального контролю від людини автоматизованим системам та алгоритмам. Впровадження алгоритмічних форм управління, заснованих на використанні великих даних, збільшує масштаби моніторингу за населенням та зміщує владну логіку на контроль і конструювання думок, формування потреб, спонукання до вчинення дій відповідно до запропонованих норм поведінки. Така автоматизація та алгоритмізація, за результатами дослідження, не позбавлена упередженості притаманній людині, оскільки алгоритми навчаються на підставі рішень, які приймаються людиною.

Як встановлення норм та правил вважається необхідною умовою життєдіяльності будь-якого суспільства, так і можливість застосування примусу є необхідним засобом упорядкування відносин у цифровому суспільстві. Вони не можуть зберігати стійкість без застосування санкцій у разі порушення прийнятих норм поведінки. Застосування покарання в цифровому суспільстві має інший характер, ніж у реальному світі. За визначенням І. Оргада в цифровому суспільстві санкції або примус застосовуються без прямого фізичного впливу на суб'єкта, шляхом застосування обмеження на вчинення дій у програмі та на платформі. Архітектура платформи, користувацька угода можуть передбачати видалення суб'єкта за вчинення порушень, передбачених законодавством та правилами платформи. Оскільки в цифровому суспільстві громадянство є віртуальним, примус здійснюється шляхом застування налаштувань платформ, оминути або обійти які може лише фахівець у сфері програмування. За визначенням науковця, віртуальна або глобальна особа налаштована, так би мовити, «запрограмована» на підпорядкування рішенням спільноти та розробників платформ. Застосування програмного коду для обмеження та блокування користувачів у цифровому суспільстві несе характер «абсолютного примусу» та виключення зі спільноти [728, с. 353]. Недотримання подібних правил та звичаїв цифрового середовища призводить до відчуження та

обмеження комунікації, зниження рівня взаємодії та співпраці цифрової особи з учасниками. Можна порівнювати обмеження та виключення з участю в цифровому середовищі, з втратою цифрового громадянства та цифровою смертю в мережі «Інтернет».

Відтак у цифровому середовищі репутаційний капітал стає цінним активом та може ставати умовою для придбання товарів, отримання послуг та робіт. Наразі це спостерігається на досвіді КНР, де застосовується система соціального кредиту та використання соціальних мереж, де «лайки» є одним із відображень лояльності, довіри та соціального рейтингу суб'єкта, не лише у віртуальному, а й у фізичному світах. Допоки цифрове громадянство надає деякі переваги, зокрема здатність впливати та ухвалювати рішення, отримувати вигоду, воно становитиме цінність, мотив прийняття та збереження статусу користувача. Цифрова репутація в КНР, яка відображається в рейтингу, стає регулятором, уособлюючись у програмному коді, який визначає обсяг доступу до тих чи інших благ у фізичному та цифровому середовищі.

Мережева структура суспільства особливо стала відчутна під час поширення Covid-19, коли органи державної влади з метою попередження поширення пандемії стали використовувати цифрові засоби для контролю за населенням. Фактично за декілька місяців карантинних обмежень у більшості держав світу стали широко використовуватися технологічні засоби контролю за населенням. Застосування подібних заходів контролю ставить питання органам, уповноваженим отримувати доступ до зібраних та згенерованих даних. Адже цифровізація суспільства, розвиток технологій інтернету, речей, розумних міст потребує постійного збору, обробки актуальних персональних даних фізичних осіб, що порушує питання пошуку балансу дотримання прав фізичних осіб та розвитку інновацій. Адже персональні дані, будучи «новою нафтою» сучасних інформаційно-комунікаційних технологій, збираються, обробляються як державними установами та організаціями, так і приватними компаніями. Означене порушує питання необхідності відмежування обробки персональних даних у залежності від інтересів обробки: для реалізації публічних інтересів та

комерційних інтересів приватного сектору. Стрімке поширення Covid-19, прискоривши впровадження нових інформаційних технологій соціального контролю, знизило «суспільну чутливість до порушення приватних кордонів задля забезпечення безпеки суспільства. Через потребу оперативного реагування на поширення Covid-19, були внесені зміни в законодавство щодо збору, обробки чутливих персональних даних та змістили баланс між дотриманням засад приватності та забезпеченням публічних інтересів здоров'я та безпеки населення[218, с. 60]. Свого часу Б. Латур зазначав, що пандемія є гарною ілюстрацією функціонування ANT, свідченням втручання в персональний простір, яка змусила похитнути баланс та прибрати бар'єри між приватним життям та суспільними інтересами.

Масове оцифрування більшості повсякденних процесів життя призводить до запровадження нових форм соціального контролю. М. Фуко підтверджує тезу, що влада за допомогою взаємопов'занного апарату управління, норм права, інформаційно-комунікаційними технологіями, соціальними нормами реалізовує форму дисциплінарної влади, спрямовану на те, щоб застосовуючи позитивні та негативні санкції, створювати в населення певні звички, очікування та стимулювати дотримання прав та норм дисципліни. Запровадження такого контролю потребує постійного оновлення даних, яке забезпечує органам державної влади можливість підтримувати нагляд. Діяльність цифрових платформ зі збору, обробки даних сприяє нагляду за фізичними особами. Поряд із зручністю та легкістю застосування цифрових платформ, автоматизація дозволяє створювати мережу, яка здійснює нагляд, подекуди не очевидний. Наразі суспільство майже перебуває в реаліях нового паноптикуму, де людина стає об'єктом постійного спостереження [259, с. 40]. Паноптикум може використовуватися не лише для контролю за фізичними особами, невпинно збільшуючи обсяги даних, які збираються цифровими платформами. Поряд із цим органи державної влади використовують новітні технології відеоспостереження для забезпечення безпечного середовища, попередження правопорушень та контролю за значними масами населення. За визначенням

М. Фуко, «суспільство безпеки», будучи технологіями контролю, має на меті не встановлення заборон або приписів поведінки, а спрямоване на дотримання обсягів девіантної поведінки на гранично допустимому рівні.

Єдиним способи уникнути паноптикуму, залишається відключення всіх пристроїв, підключених до мережі «Інтернет», що вимагає жертвувати благами інформаційного суспільства. Проте участь у цифровому середовищі стає умовою здійснення фундаментальних прав через зростання кількості державних послуг, отримання яких вимагає доступу до цифрових платформ.

В умовах потужної глобалізації, соціально-економічна, політична та культурна структури пронизується інформаційними зв'язкам, які в сукупності з акторами і складають мережу, що характеризується взаємопов'язаністю та децентралізацією. Поширення COVID-19 та введення воєнного стану в України посилило гібридизацію між віртуальним та фізичним світами, підштовхнуло прискорити процес розвитку електронного урядування в Україні та інших видів соціальної взаємодії в інтернеті як єдиного безпечного середовища [235, с. 86].

Зростання кількості державних послуг та діяльності, яка потребує підключення до мережі «Інтернет», цифрового профайлу (акаунту) фізичної особи, розвиток технологій обробки великих даних, інтернету речей, транскордонної передачі персональних даних, віддаленої біометричної ідентифікації, прискорення темпів цифровізація суспільства – загострюють проблему ідентичності. Відтак ідеалістичним уявленням про вільний від втручання державної влади цифровий світ «користувачів у хмарах» протиставляється світу організованих мережевих структур та ієрархій.

Наразі із силою, якою володіють атоми та віруси в розумінні ANT, можна порівняти вплив, який здійснюють на людину у фізичному світі результати профілювання (на основі яких приймаються доленосні рішення), відгуки та коментарі (позитивні або негативні), лайки, завантажені фото та відео інших користувачів із фізичною особою, які ладні впливати, підіймати (знижувати) рейтинги та формувати цифрову репутацію в мережі «Інтернет».

Змінився процес формування цифрової репутації, оцінювання популярності та вплив у мережі вийшов за межі комунікаційних платформ, багатокористувацьких ігор та поширився на платформи та майданчики для працевлаштування. За твердженням А. Аграваля, змінився підхід до працевлаштування та оцінки трудової діяльності. Відтак цифрова репутація та репутаційна економіка відіграє істотну роль у цивільних відносинах, змінюючи процес пошуку контрагентів, найманих працівників та підходи до оцінювання якості товарів, робіт, послуг тощо [295, с. 219].

Відбувається переосмислення соціальних взаємозв'язків та соціального капіталу як мережі контактів особи, що забезпечують їй доступ до ресурсів. Наразі цифрова репутація визначається не лише кількістю «слабких зв'язків», а оцінюється алгоритмами, що перетворюють відгуки минулих контрагентів та роботодавців на кількісно виміряну репутацію. Технології та соціальні мережі дозволяють замінити необчислювальну «хмарну» довіру на вимірювану, математично обчислювальну прозору репутацію, доступну користувачам. Репутація в мережі стає вимірюваним ресурсом, який підлягає управлінню, а платформи надають доступ користувачам до математичного розраховування її показників. Цифрова репутація розміщується на платформах третіх сторін, розподіляється нерівномірно, характеризуючи користувачів та постачальників товарів, робіт, послуг.

На думку К. Делларокаса, відбувається «цифровізація сарафанного радіо», що призводить до того, що цифрова репутація та створювана нею прозорість стимулює сумлінну поведінку фізичних осіб та компаній в умовах прозорого цифрового середовища. Дана властивість стає чинником для заохочення до співпраці з незнайомими користувачами в мережі [471, с. 1407].

Враховуючи викладене, процеси цифровізації та посилення мережевої структуризації суспільства призводить до переосмислення становища людини не лише в юриспруденції, а й філософії, психології та соціології. Цифровізація має сприйматися не як ціль, а як засіб досягнення благополуччя та злагоди суспільства. Поряд із викликами, обумовленими розвитком IoT та застосуванням

автоматизованих систем, які можуть призводити до втручання та порушення недоторканності приватного життя, створення цифрових диктатур, мережева структура може сприяти співробітництву міжнародних організацій та держав у сфері прав людини для подолання цифрового розриву, розробки єдиних людиноцентристських підходів та принципів застосування автоматизованих систем та правового регулювання мережі «Інтернет».

2. ДОКТРИНАЛЬНІ ТА ПРАКТИЧНІ ПІДХОДИ ДО ФОРМУВАННЯ ЦИФРОВОЇ ІДЕНТИЧНОСТІ В МЕРЕЖІ «ІНТЕРНЕТ»

2.1. Концептуальні підходи до визначення права на цифрову ідентичність у мережі «Інтернет»

Інтернет змінює сприйняття навколишнього світу, ставши невід'ємним елементом комунікації, державного урядування, освіти тощо. Враховуючи те, що у віртуальному світі стають доступними інструменти, недоступні у фізичному світі, це неминуче впливає на конструювання ідентичності фізичної особи в мережі «Інтернет» [666, с. 10].

Один із прибічників «вільного інтернету», американський письменник Дж. П. Барлоу в «Декларації незалежності кіберпростору» зазначив, що традиційна для права категорія «особа» не застосовувана до відносин в мережі Інтернеті [294].

У глобальному віртуальному просторі всі досягнення культури трансформуються в тексти, діалоги, знаки, образи, особа не є виключенням, являючи собою єдність образу та тексту, в такому вигляді представляє себе через посередництво свого alter ego – цифровий образ, цифрову проєкцію або профіль.

Відтак невід'ємною складовою розвитку цифрового суспільства стає застосування цифрового профілю фізичної особи.

Наразі наука та правотворча практика не характеризуються єдністю в застосовані категоріального апарату. Для позначення фізичної особи в мережі «Інтернет» у науковій літературі засовуються такі терміни як «віртуальна ідентичність», «цифрова ідентичність», «віртуальна особа», «цифровий електронний профіль особи», «цифровий електронний профіль людини», «аватар», «актор» тощо [239, с. 64]. Дослідження даного питання має практичне значення, адже пов'язане із встановленням обсягу правосуб'єктності фізичної особи у віртуальному просторі, аналогічно як у фізичному світі, визначенням обсягу прав та обов'язків особи та захисту в даному просторі [811]. Тому постає

потреба у співвідношенні вказаних понять та розгляду можливості встановлення їх тотожності.

З огляду на істотне поширення категорії «віртуальна» або «цифрова ідентичність», доцільно звернутися до розуміння ідентичності в законодавчих актах. Хоча поняття «ідентичність» «не передбачено в Конвенції про права дитини, у ст. 8 Конвенції передбачає право на ідентичність та елементи ідентичності, що держави-учасниці зобов'язуються поважати право дитини на збереження індивідуальності, включаючи громадянство, ім'я та сімейні зв'язки, які передбачаються законом, не допускаючи незаконного втручання [443].

Конвенція про права дитини підтверджує право на ідентичність відповідно до міжнародного права, водночас стосується неповнолітніх та має обмежене застосування. У свою чергу ЄСПЛ у своїй практиці зазначає, що право на ідентичність відносно повнолітніх та неповнолітніх підлягає захисту відповідно до норм ЄКПЛ [401].

Право на ідентичність може бути виведене шляхом аналізу низки рішень ЄСПЛ. Право на ідентичність захищає такі елементи ідентичності як ім'я, прізвище, право знати походження, стать чи етнічну приналежність, що розкрито в рішеннях Godelli v. Італії[387], Mikulić v. Croatia [395], Odiëvre v. France [399]. Завдяки розвитку права на ідентичність, до нього були включені такі елементи ідентичності як образ та громадянство Relu Adrian Coman and Others v. Inspectoratul General pentru Imigrări and Ministerul Afacerilor Internet, 2018 [407]. На думку Є. Міхалкевич-Кадзела та Є. Мільчарека, зміст права на ідентичність перебуває в розвитку та трансформації, тому до її складу поступово включаються нові елементи ідентичності, такі як свобода вибору зовнішнього вигляду, гендерна та інтернет ідентичності [666, с. 3].

На думку К. Салівана, право на ідентичність (науковець розглядає ідентичність відповідно до Закону про посвідчення особи Великобританії) є не лише правом контролювати персональну інформацію, а й визнання того, що кожна особа володіє невід'ємним інтересом у власній унікальності. У контексті національної системи ідентифікації Великобританії, яка вимагає ідентифікацію

особи для укладення правочину, право на ідентичність означає право людини бути визнаною та право укладати правочини як унікальний суб'єкт. Закон про посвідчення особи Великобританії накладає на осіб певні обов'язки відносно повідомлення про зміни та помилки даних у реєстрі, а також обмеження розкриття даних державними органами. За твердженням науковця, з огляду на те, що зареєстрована особа – це особа, яку держава офіційно визнає, то можна стверджувати про виникнення додаткових прав особи та зобов'язання держави сприяти у здійсненні цих прав [803, с.21].

К. Саліван розмежовує право на ідентичність та право на недоторканність приватного життя. Якщо право на ідентичність надає захист персональних даних суб'єкта від незаконного збору, обробки та використання іншими особами, то право на недоторканність приватного життя стосується небажаного втручання, збору, розкриття та використання персональної інформації про особу [803, с. 21].

Слід зазначити, що інтернет значний час наділяв осіб правом вільного вибору та зміни ідентичності, псевдонімів, що створювало ілюзію анонімності в мережі. Наразі ставлення до анонімності змінилося, що обумовлене вимогами ідентифікації та автентифікації, зміною масштабів обробки персональних даних. Сучасні тенденції навпаки зводяться до презентації реальної фізичної особи в цифровому просторі. Водночас поточний рівень розвитку інтернету та соціальних мереж свідчить, що платформи можуть обмежувати суб'єкта у виборі імені, вимагаючи використання автентичного імені особи на платформі та під час автентифікації.

Щоб стати суб'єктом цивільних відносин та бути притягненим до відповідальності за порушення, особа має бути належним чином ідентифікована, що наразі змінює підхід до анонімності в мережі, обмежуючи вільний вибір імен або псевдонімів.

У доктрині висувається твердження, що в мережі виникає самостійно діючий суб'єкт прав або «електронна особа», володіюча соціальним статусом, особистою та соціальною ідентичністю [829, с. 285]. На наш погляд, це твердження є свідченням термінологічного змішування таких категорій як

електрона особа та цифрова ідентичність. Адже термін «електронна особа» застосовується для позначення роботів із високорозвиненим інтелектом, які можуть мати матеріальну форму [74, с. 5; 202, с. 7]. «Електронна особа (особистість)» застосується в Резолюції Європейського Парламенту від 17 лютого 2018 року з питань цивільно-правових норм про робототехніку, якою передбачається наділення роботів, які іменуються «електронною особою (особистістю)» низкою прав та обов'язків [706].

У результаті створення акаунту, в мережі не виникає новий суб'єкт права, за профілем «ховається» фізична або юридична особа, якій належать всі набуті права та обов'язки. Отже, учасниками цивільних правовідносин у мережі залишаються ті ж суб'єкти права – фізичні та юридичні особи, які лише здійснюють свої права та обов'язки за допомогою віртуальних проєкцій, створених у мережі [829, с. 281]. Цифрова ідентичність представляє та ідентифікує певну фізичну особу.

У зарубіжних джерелах поряд із терміном «віртуальна ідентичність» використовується термін – «цифрова ідентичність» у тотожних значеннях. З огляду на те, що розуміння слова «віртуальний» стосується явищ, які не існують у фізичному світі та є вигаданими [846], то «віртуальна особа» може бути визначена як така, що не існує у фізичному світі. Уявляється, що використання такого словосполучення є не коректним та більш доцільним є застосування «цифрова ідентичність» або «цифрова особа». Натомість «цифровий» дослівно тлумачиться як позначений або виражений цифрами. Крім того, Світовий Банк Реконструкції та Розвитку застосовує саме термін «цифрова ідентичність» для позначення записаних в електронному вигляді даних, які дозволяють однозначно ідентифікувати особу [807]. Відтак під «цифровою ідентичністю» пропонується розглядати ідентичність фізичної особи в мережі, яка має чітко окреслену фізичну ідентичність зі своїми унікальними характеристиками, зареєстрованими в системі реєстрації в конкретній державі, яку можна ідентифікувати. Цифрова ідентичність не є суб'єктом права, не приймає вольових рішень, не володіє правосуб'єктністю та не може від власного імені виступати учасниками тих чи

інших правовідносин, а є продовженням фізичної особи в мережі, представляє користувача в онлайн-середовищі [228, с. 35; 213, с. 406]. Тому для позначення фізичної особи як суб'єкта права в мережі пропонується використовувати саме термін – «цифрова особа або ідентичність». Разом з тим, у роботі терміни «віртуальна ідентичність» та «цифрова ідентичність» використовуються як тотожні, та під час посилань на зарубіжні джерела залишена термінологія, використана їх авторами.

Я. Коксвік розуміє під віртуальною особою: проєкцію особи, представлену в мережі, яка використовується під час спілкування; опубліковані дані та бажану роль фізичної особи у спілкуванні [844, с. 506]. За визначенням Я. Коксвіка, закон має взяти на себе ту ж місію, що і в реальному світі щодо визначення правового становища віртуальної особи у віртуальному середовищі, прийняття заходів, які б не допускали дискримінацію, забезпечували рівний обсяг прав та обов'язків у віртуальному середовищі та фізичному світі [843, с. 32].

В.Н. Мортеза розглядає віртуальну ідентичність як презентацію фізичної особи, яка може співпадати або не співпадати з ідентичністю фізичної особи в разі створення вигаданої, фейкової віртуальної особи. На думку науковця, юридичне визнання цифрової особи має передбачати право кожного суб'єкта володіти посвідченням особи у віртуальному просторі поряд із традиційним паперовим посвідченням та свідоцтвом про народження. Науковець розуміє під юридично визнаною ідентичністю – ідентичність офіційно визнану державою для набуття юридично значущих прав та здійснення обов'язків. Якщо людина не визнана юридично як суб'єкт права, вона не може брати участь в юридично значущих діях, набувати прав та обов'язків для себе, виступати представником, стороною договору. Такі правила мають застосовуватися по відношенню до цифрового середовища [675, с. 6].

Поряд із поширеною позицією, що віртуальну ідентичність формують персональні дані про фізичну особу як віртуальний або «цифровий» образ (nickname, мережеве ім'я), IP-адреса в мережі «Інтернет», висувається точка зору, що розуміння віртуальної ідентичності не вичерпується цими ознаками.

Так, С. Кроуфорд зазначає, що розуміння ідентичності є значно ширшим, ніж механічна діяльність із ідентифікації особи та включає інші складові. Особа, яка сприймається іншими (в іграх: віртуальних світах) є ідентичністю цієї особи, так само ця ідентичність формується у взаємодії та внаслідок комунікації з іншими особами під час дискурсу. Тому з ідентичністю тісно пов'язана репутація, будучи сформованою певною групою та в певному контексті [445, с. 4]. Дана позиція свідчить, що зміст цифрової ідентичності не вичерпується лише персональними даними. На думку С. Кроуфорда, ідентичність є колективним (груповим) проєктом, що створюється в умовах, в яких діє особа, яка підлягає ідентифікації. В аватара (науковець не проводить різницю між цифровою ідентичністю та аватаром) є визначені характеристики, зв'язки (відносини) та інтереси, які виникають внаслідок його пригод у визначених світах, які взяті разом як «хмара» репутації, досвіду та об'єктивних чинників, складають його «ідентичність», яку неможливо передбачити в момент її народження або (створення) аватару.

С. Кроуфорд дотримується позиції, що юриспруденція передбачає механізми захисту прав та інтересів особи, які не відповідають динамічності віртуального світу. З цієї причини науковець ставить під сумнів ефективність правового регулювання в разі прийняття єдиного міжнародного або національного акта стосовно ідентичності. Категорія «ідентичність» потребує єдності науковців щодо її розуміння. Так може виявитися деструктивним прийняття правил та норм для всього віртуального світу, які б передбачали видалення ідентичності за вчинення порушення [445, с. 4]. Науковець ставить під сумнів ефективність прийняття норм, які б передбачали відповідальність за порушення умов віртуальних світів та розмірковує над ідеєю міжнародного онлайн-суду, уповноваженого розглядати справи про застосування санкцій та видалення ідентичності (аватарів).

Аналогічної позиції дотримуються вітчизняні правники. А. Кравченко розглядає «цифрову ідентичність» як досить широку категорію, яка охоплює всі дані про особу, що зберігаються в інформаційному просторі, включаючи дані конфіденційного та особистого характеру, персональні дані та дані про

взаємодію особи в інтернеті, персональні дані, які можуть бути зібрані без відома особи [87]. У такому розумінні поняття «цифрова ідентичність» тісно пов'язано з категорією «цифрового сліду» (digital footprint), під якою розуміються: мітки геолокації, фото, відео, повідомлення, пошукові запити, паролі, номери банківських карток, публікації в соціальних мережах, інші дані, які залишаються в мережі.

Є.О. Харитонов та О.І. Харитонова розуміють під цифровою особистістю особливе поєднання імені, дати народження, місця проживання, електронної пошти та сторінок, представлених записів, фото, відео та особистих соціальних зв'язків, біометричних даних, які можуть бути використані для представлення особи в цифровому, віртуальному світі. Тобто певної системи інформації, цифрових даних, які є цифровою ідентичністю (особистістю) з відповідним правовим статусом об'єкта права. Відомі українські правники зазначають, що поряд із цифровою особистістю, категорія цифрова людина є суперечливою. Запропоновані в літературі характеристики такої особи не свідчать про появу нових ознак, порівнюючи із С. Хокінгом, який спілкувався за допомогою комп'ютера, залишався людиною, звичайним суб'єктом права [265, с. 6].

Аналогічне твердження висуває Г. Терпстра, що ідентичність є сукупністю інформації, яка включає дані про взаємодію профілю з іншими за допомогою цифрових профайлів, та про дії, вчинювані особою в мережі. А пропонований системою контент є результатом накопиченого досвіду цифрової ідентичності в минулому [811, с. 8].

А. Сарма та Х. Жірао дотримуються аналогічного підходу, що цифрову ідентичність слід розглядати як суму конструктів, що описують її сутність. [780, с. 353] Цифрову ідентичність формує не лише сума офлайн-ідентифікаторів – персональних даних – а також вся сукупність властивостей об'єкта, які генеруються системою IoT, характеризують та описують особу. [520, с.3]. Пристрої та сервіси IoT генерують дані, які можуть бути перетворені на інформацію, що характеризує суб'єкта даних.

Дотримуючись такого підходу С. Вахтер зазначає, що як сама людина (тобто те, як вона себе сприймає та розуміє), так і зовнішні суб'єкти (наприклад, провайдери соціальної мережі,) формують цифрову ідентичність людини та управляють нею. Користувач може залишатися необізнаним про повний обсяг та властивості цифрової ідентичності, оскільки інформація, що становить цю ідентичність, може бути сконструйована ззовні (тобто за допомогою аналізу)[851, с. 436]. Користувач може видаляти публікації на сторінці. Видалення минулих публікацій у соціальних мережах, які перестають відповідати іміджу, з метою контролю та управління цифровою ідентичністю отримало назву «білої стіни». Водночас інтернет зберігає всі дані на серверах, а видалення публікацій, повідомлень, світлин призводить лише до того, що їх перестають бачити користувачі, які відвідують сторінку, та не призводить до видалення даних із акаунта та цифрової ідентичності. В означеному принципі проявляється ідея того, що цифрова ідентичність може існувати вічно в мережі [811, с. 8].

Зовнішні системи (провайдери, соціальні мережі, системи IoT) збирають персональні дані, характеристики використання та вчинки в мережі, які аналізуються системою ШІ та конструюють цифрову ідентичність особи. Технології ідентифікації допомагають організувати зовнішнє управління цифровою ідентичністю. На думку Л. Флоріді, користувач може не володіти повним контролем за змістом власної цифрової ідентичності, адже зміни можуть відбуваються у профілі через постійну обробку персональних даних та даних про взаємодію з користувачами [520, с. 8]. С. Вахтер висловлює позицію, що користувач може бути необізнаним щодо підстав, обґрунтованості зроблених висновків щодо нього та не мати можливості їх оцінити [851, с. 436]. Така ситуація є наслідком того, що в результаті профілювання персональних даних автоматизованими системами в мережі, згенеровані характеристики користувача йому не розкриваються. Користувач залишається в невіданні, які дані про нього генеруються системою IoT, платформами та соціальними мережам. Для зміни такої ситуації, із прийняттям Регламенту ЄС 2016/679 [700], було закріплено

право на доступ до даних, право на внесення змін до неточних первинних даних та внесення змін у результати профілювання. Іншими словами, внаслідок профілювання конструюється та трансформуються дані про користувача, які стають частиною його цифрової ідентичності та формують майбутнє ставлення до нього в системі IoT та в інфосфері. Л. Флоріді під інфосферою, або інформаційним середовищем розуміє контекст, утворений системою інформаційних об'єктів, включаючи всіх агентів, об'єкти та взаємовідносини [520, с.7].

Досліджуючи етимологічне значення ідентичності, М. Панебянко звертає увагу на те, що ідентичність, будучи властивою кожній фізичній особі, включає гідність та репутацію[732, с. 5]. Слід звернути увагу, що цифрова репутація є дійсно широкою категорією та може містити кредитну історію, кредитний рейтинг особи тощо.

Разом з тим, ми не поділяємо позицію науковців, які розглядають цифрову репутацію як складовий елемент цифрової ідентичності, дотримуючись точки зору, що цифрова репутація має бути визнана окремим особистим немайновим благом, охоронюваним цивільним законодавством, що й буде розглянуто далі.

Позиція, що категорія «ідентичність» не вичерпується певною низкою персональних даних, була висунута Є. Гоффманом у роботі «Уявлення себе у повсякденному житті» 1969 року, де він визначив ідентичність як низку вчинків, в яких застосовується «управління враженнями», що зображують та виражають особу в різних середовищах. Ідентичність певною мірою контролюється особою, але переважно ідентичність формується світом, у якому особа вчиняє дії [436, с. 6]. На думку науковця, особа володіє декількома ідентичностями.

Слід уточнити, що особа може володіти цифровими профілями в інтернеті, зареєстрованими в різних системах, кількість яких наразі необмежена. У такому вузькому розумінні категорія «цифрова ідентичність» співпадає із цифровим профілем (акаунтом), який створюється особою кожного разу при реєстрації в будь-якій інформаційно-комунікаційній системі. На шляху сингулярності єдиний цифровий профіль може поступово об'єднувати персональні дані з різних

інформаційних систем [241, с. 35]. Означена тенденція проявляється у прагненні компаній розробити програмну архітектуру, яка сприяє створенню єдиної автентичної цифрової ідентичності, а з тим і єдиного цифрового профайлу.

Як зазначає М. Хільдебрант, в умовах корпоративного та глобального управління, застосування та удосконалення надійних засобів ідентифікації, значення цифрового профілю зростає, стаючи невід'ємною умовою здійснення прав особи в різних сферах у мережі [558, с. 55].

Т. Смедінгоф розуміє цифрову ідентичність як особу, яка опосередкована участю та використанням комп'ютерних технологій або цифрових комунікацій, таких як цифрові медіа та інтернет [792].

Ф. Джордж, А. Сіль дотримуються вузького підходу до цифрової ідентичності, яка є результатом активної діяльності особи для досягнення певної мети, ототожнюючи обліковий запис (акаунт) та цифрову ідентичність [531].

Із формуванням єдиної цифрової ідентичності пов'язується реалізація принципу пов'язаності акаунтів та персональних даних, який має дозволити користувачам (державним органам, органам місцевого самоврядування) отримувати доступ та обробляти необхідні дані по мірі автоматичного оновлення та об'єднання роз'єднаних даних в єдиному цифровому профілі [531].

Слід погодитися з науковцями в тій частині, що електронний цифровий профіль може створюватися для представлення не лише фізичної особи в мережі. Наприклад, коли за профілем «ховається» нейронна мережа або інтелектуальний програмний агент. Автоматизовані системи наразі вчиняють правочини та дії, на вчинення яких їх налаштував користувач. Нейронні мережі можуть надавати пропозиції щодо варіантів вчинюваних дій та поведінки для подальшого схвалення користувачем.

Цифровий профіль людини створюється шляхом внесення персональних даних під час реєстрації на майданчиках, сайтах, або коли особа залишає коментарі на сайтах тощо. Фізичні особи за допомогою цифрового профілю вчиняють юридично значущі дії: купівлю-продаж товарів, замовлення послуг, робіт, публікація та оприлюднення об'єктів авторського права та використання

інших об’єктів інтелектуальної власності в мережі. Поступово делегують повноваження автоматизованим системам (інтелектуальним агентам) проведення регулярних переказів, купівлю-продаж цінних паперів, шляхом налаштування автоматичного списання платежів. У науці дискутується питання здатності інтелектуальних агентів приймати вольові рішення та рішення не в інтересах людини. Існують певні побоювання, що по мірі розвитку ШІ, цифровий профайл зможе відокремитися від фізичної особи, стати автономним, власними діями набувати прав та обов’язків, укладати правочини, які вірогідно можуть буті не інтересах фізичної особи, розробника.

Наразі інтелектуальні агенти та цифровий профіль є невіддільним та виражає волю фізичної особи. Завдання, які виконує інтелектуальний агент, навіть в автономному режимі, обмежуються лише налаштуваннями користувача та метою, заради якої він був створений.

Огляд наданих визначень цифрового профайлу дозволяє стверджувати, що під цифровим профайлом фізичної особи розуміється акаунт (обліковий запис, профіль) фізичної особи в певній інформаційно-комунікаційній мережі. Цифровий профіль або акаунт у мережі «Інтернет» постає як цифровий образ, створений людиною шляхом внесення персональних даних та реєстрації. Під акаунтом у соціальній мережі розуміється особиста сторінка, на якій користувач розміщує особисту інформацію, відео, аудіо та інші матеріали, за допомогою якої веде листування з іншими користувачами, та управління якою можливе лише після процедури авторизації, шляхом введення відповідного логіну та пароля [117, с. 60]. Тобто акаунт (обліковий запис) являє собою систему даних про користувача, необхідних для автентифікації та надання доступу до персональних даних або налаштувань.

У науці висувається теза про закріплення на законодавчому рівні положення про обов’язкову відповідність електронного профайлу конкретній особі у фізичному світі та що таке положення не переслідує запровадження контролю держави за фізичними особами у мережі, а ґрунтується на меті запобігання порушенню прав фізичних осіб через поширення використання

цифрових профайлів. Безумовно таке твердження носить досить суперечливий характер, адже як свідчить досвід КНР, де умовою використання мережі є авторизація відповідно до національного номеру телефону, який можна оформити за наявності документів, що посвідчують особу, то такі умови несприятливо впливають на вільне вираження.

Персональні дані цифрового профілю складають інтерес для фінансових установ та платформ електронної комерції. За результатами обробки персональних даних проводиться профілювання з метою ефективного та персоналізованого надання послуг. Крім того, використання цифрових профілів є зручним інструментом для користувачів.

Слід зазначити, що окремими недоліками визначень цифрового профілю, які надаються в доктрині, що зміст цифрового профілю особи складають лише дані, які ідентифікують її у відповідних системах державних органів. Тож визначення цифрового профілю обмежується сферою електронного урядування, а інформація про особу, яка представлена в соціальних мережах, розміщена на платформах електронної комерції тощо, не береться до уваги. Фактично подібні визначення дозволяють говорити, що будь-які дані в системах про фізичних та юридичних осіб є цифровими профілями [829, с. 285].

Особливістю формування та введення електронного цифрового профілю людини в інформаційних системах органів державної влади та місцевого самоврядування є вимога достовірності та актуальності даних, а такий профіль у державній інформаційно-комунікаційній системі не може бути симуляцією або представляти вигаданого суб'єкта. Збір та обробка даних має здійснюватися лише відповідно до законної мети. Наразі законодавство окремих держав як Корея, КНР вимагає проведення ідентифікації та автентифікації відповідно до національних посвідчень, навіть у недержавних інформаційних системах – соціальних мережах, іграх та метасвітах [609].

Слід зазначити, що цифровий профіль генерується як у державних, так і приватних інформаційних системах, а збір та обробка персональних даних можуть здійснюватися лише відповідно до законної мети, для якої суб'єкт надав

персональні дані. Обов'язковою умовою формування цифрового профілю в державних та фінансових системах є достовірність та актуальність персональних даних фізичної особи. Висловлюється думка щодо створення цифрового профілю, який зв'язується виключно з інформаційними системами державних органів [829, с. 285]. З такою позицією складно погодитися, адже цифровий профіль (акаунт) може створюватися особою як у державних інформаційних системах, так і приватних, як соціальні мережі.

Торкаючись питання, які саме дані мають складати зміст цифрового профайлу, слід зазначити, що наразі в науці не існує єдиного підходу щодо даних, які б мали бути включені. Окрім персональних даних, що містяться в посвідченні особи громадянина (паспорті), цифрова ідентичність фізичної особи в системах державних органів може містити дані банківських рахунків, медичних, пенсійних установ, ідентифікатори податкових органів, дані про автотранспортні засоби, дані з державного кадастру, про освіту, дані соціальних мереж тощо.

У доповіді An Introduction to Online Platforms and their Role in Digital Transformation у 2019 році визначені такі види персональних даних, які збираються компаніями: персональні дані, які добровільно надаються користувачами (інформація, що добровільно надається користувачами під час ідентифікації, реєстрації на майданчиках електронної комерції); персональні дані, отримані на основі інформації про поведінку користувача (наприклад, дані про проведений час у мережі); персональні дані, отримані в результаті аналізу первинних персональних даних (наприклад, розрахунок кредитних балів на підставі аналізу укладених договорів купівлі-продажу на майданчиках електронної комерції) [308].

З урахуванням вищевикладеного, поняття цифрової ідентичності визначається як досить широка категорія, може не вичерпуватися персональними даними особи та даними цифрового профілю в державних, фінансових та приватних інформаційних системах, включати всі дані, які особа залишає в мережі «Інтернет» під час користування та взаємодії, які охоплюються

поняттям «цифровий слід»[829, с. 285]. Разом з цим, визначення категорії «цифрова ідентичність», має чітко окреслені межі, що обумовлено метою цифрової ідентичності – проведенням ідентифікації або тотожності фізичної особи в мережі, що буде розглянуто далі.

Д.Дж. Солове, досліджуючи проблеми приватності в США, висуває категорію «цифрового досьє», яке за змістом та значенням близьке до розуміння «цифрової ідентичності», що охоплює усі дані стосовно фізичної особи, незалежно від того, де вони не зареєстровані або опубліковані. Д.Дж. Солове порівнює їх із «електронним колажем», який охоплює більшу частину життя людини зафіксовану в записах у мережі[798, с. 15].

К. Саліван провів дослідження цифрової ідентичності з урахуванням системи національних посвідчень та національного реєстру ідентифікаційних даних за законодавством Великобританії та Австралії [803, с. 20]. Науковець обґрунтовує поширення цифрової ідентичності у зв'язку використанням майданчиків електронної комерції, електронним урядуванням та ін. Поряд із цифровою ідентичністю, під якою розуміється вся інформація, зареєстрована в цифровій формі про фізичну особу, яка доступна в системі або реєстрі, науковець виокремлює так звану «ідентичність транзакцій», яка є складовою частиною цифрової ідентичності, під якою розуміються певні дані (ПІБ, дата народження, стать і підпис та/або цифровий ідентифікатор), що ідентифікують особу під час вчинення правочину. Ідентифікаційні дані для транзакцій порівняно статичні, більша частина інформації встановлюється під час народження, включаючи: ім'я, дані про народження, підпис, фотокартку, біометричні дані. Науковець відрізняє ідентичність необхідну для укладення правочину або «Ідентичність транзакцій» та цифрову ідентичність, яка включає дані про особу, які містяться в національних реєстрах та необхідні для вчинення правочину. «Ідентичність транзакцій» складають також інші персональні дані профілю, що доповнюється та оновлюється, створюючи історію правочинів [804, с. 562].

На думку науковця, «ідентичність транзакції» виконує традиційні функції посвідчення. Водночас на відміну від традиційних документів, що засвідчують

особу, визначальне значення при дистанційному вчиненні правочину здійснює система, а не фізична особа. Виконання правочину забезпечується не сторонами, а інформаційною системою [804, с. 566]. Ідентифікаційні дані сторін можуть бути надані сторонами дистанційно, а виконання правочину забезпечено функціонуванням інформаційної системи, у разі успішної автентифікації сторін правочину.

На погляд К. Салівана, функції «ідентичності транзакцій» відображені у процесі проведення ідентифікації та автентифікації. Ідентифікаційні дані, зібрані під час реєстрації, використовується для проведення автентифікації фізичної особи. Такі ідентифікаційні дані розглядається як «ідентичні чи нерозривно пов'язані з фізичною особою». Ідентифікаційні дані «ідентичності транзакцій», за визначенням науковця, складають певний обсяг даних, які збираються про фізичну особу в мережі «Інтернет» та є складовою цифрової ідентичності.

Враховуючи викладене, можна стверджувати, що «ідентичність транзакцій» або ідентичність необхідна для укладення правочинів у розумінні К. Салівана за змістом є близькою до розуміння аканту, який створюється фізичною особою під час реєстрації на платформі та використовується для укладення правочинів, отримання доступу до даних у мережі. К. Саліван порівнює визначення цифрової ідентичності з цифровою особою, запропонованою Д. Дж. Соловом. На відміну від «цифрової особи» Д.Дж. Солове, яка включає всі дані про особу в мережі, «цифрова ідентичність» К. Салівана охоплює дані про фізичну особу, що містяться в національних реєстрах та необхідні для вчинення правочину відповідно до законодавства Великобританії та Австралії [798, с. 20].

На думку К. Саліван, у загальній системі права поняття фізичної особи залишається досить розмитою категорією, оскільки в договірному праві категорії ідентичність не приділяється достатньої уваги, а акцент ставиться на наявності зустрічності волевиявлення сторін для укладання договору, поінформованості сторін, досягнення домовленості та особистій участі сторін. Така ситуація є результатом практики XIX і XX століть, що призвела до невизначеності ролі ідентичності в господарських договорах. На погляд науковця, у зв'язку із

застосуванням дистанційних методів ідентифікації та укладення правочинів, привертає увагу дослідження концепції ідентичності в науці [804, с. 557].

По мірі того як особисте вчинення правочинів заміщається дистанційним вчиненням правочину, яке не вимагає особистої присутності, зростає значущість забезпечення автентифікації та ідентифікації. Значення цифрової ідентичності також зростає у зв'язку із цифровізацію державних послуг, що трансформує способи взаємодії органів місцевої та державної влади з фізичними особами. Укладення правочинів у мережі актуалізує значення цифрової дистанційної ідентифікації на безпрецедентний рівень значущості. К. Саліван проводить розмежування між ідентифікацією та ідентичністю. Окремі персональні дані можуть виступати ідентифікаторами особи, мають обмежене використання для ідентифікації особи. Так, лише ім'я не є унікальним та не виділяє фізичну особу з-поміж решти осіб. Ідентифікація – це лише один із двох процесів, що використовуються для встановлення ідентичності при вчиненні транзакції. Основна ж роль ідентифікаційних даних полягає в тому, щоб пов'язати зареєстровану цифрову ідентичність з фізичною особою[804, с. 557]. Науковець, підсумовує, що право на ідентичність має включати виключне право особи використовувати власну ідентичність [803, с. 78].

За визначенням В.М. Мортеза, людина, користуючись інтернетом, створює власну цифрову копію, яка реалізує її права та свободи у віртуальному середовищі. А цифрові засоби та доступ до інтернету стає невід'ємною складовою сучасного життя, умовою успішного здійснення прав та обов'язків у суспільстві, отримання та замовлення послуг і робіт, придбання товарів, отримання медичних послуг (запису до лікаря, отримання електронних рецептів, укладення договорів страхування тощо), державних послуг, вираження творчості та комунікації за допомогою соціальних мереж, комп'ютерних ігор, метасвітів та ін. Відсутність комп'ютера, смартфона та інтернету може позбавити можливості отримати послугу, укласти правочин, отримати медичну допомогу, обмежити або позбавити можливості здійснення права людини (звісно, за умови, що така послуга надається лише онлайн).

Досліджуючи питання віртуальної ідентичності, В.М. Мортеза зазначає, що відбувається трансформація уявлень про категорію «фізична особа» як суб'єкта, адже у мережі «Інтернет» створюється ідентичність, яка одночасно співіснує у фізичному та у віртуальному світах [675, с. 7]. У таких умовах на перший план у цифровому просторі виходить цифрова ідентичність фізичної особи в інтернеті.

В.М. Мортеза солідаризується із позицією Ф. Джордано, що розвиток та трансформація віртуальної ідентичності не є свідченням виникнення нової сутності або ідентичності в мережі, ніж та, яка існує у фізичному світі [537, с. 8]. На погляд В.М. Мортеза, основна відмінність віртуальної ідентичності від ідентичності в реальному світі полягає у формах та особливостях виникнення віртуальної ідентичностей. Множинність ідентичностей, яка називається викликом або кризою ідентичності в кіберпросторі, є лише формою вираження ідентичністі у віртуальному світі. Множинність ідентичностей може призводити до зловживання та неправомірного використання ідентичності. Науковець вважає, що відмінністю природи, ідентичності в реальному та віртуальному світах є у відсутності нагляду за її функціонуванням зі сторони правоохоронних органів. Якщо розглядати ідентичність в синонімічному значенні «людини», то людина володіє ідентичністю зі своїми унікальними властивостями у фізичному світу. Ідентифікаційні дані такої особи зареєстровані у відповідних державних реєстрах. Можна підсумувати, що науковець розглядає цифрову ідентичність у розумінню профілю або акаунту, які створюються на платформах.

Слід зазначити, що подекуди в літературі трапляються терміни «цифровий аватар», «цифровоǐ двійник» поряд із категорією «цифрова ідентичність» як синоніми, з огляду на спільну репрезентативну складову цих понять [214, с. 294; 829, с. 283].

Водночас, на наш погляд, слід відмежовувати означені поняття та поставити під сумнів можливість застосування терміна «аватар» для позначення фізичної особи в інтернеті та використовувати як тотожне щодо таких термінів як «віртуальна особа» або «віртуальний цифровий електронний профіль». Для

цього звернемося до позначення та слів, які використовуються для конструювання терміна «аватар» у літературі.

О. Костенко під поняттям «електронний аватар» розуміє – дані в електронній формі, достатні для відтворення прототипу людини – володільця електронного аватару в метасвіті (кіберпросторі) з максимальною достовірністю та правами, встановленими законодавством [84, с. 56].

З погляду Т. Дей, [453, с. 140] аватар – вигаданий уявою витвір, який втілює фантазії, перетворені в керований об'єкт, який існує у віртуальному світі. Термін «аватар» від початку запозичений з індуїстської філософії, де під «аватаром» розумівся фізичний прояв вищої істоти у світі. Також у віртуальному світі користувач постає «вищою істотою», а аватар – є цифровим проявом користувача у віртуальному світі. Аватари можуть бути схожими на фізичних осіб у їх здатності виражати окремі емоції: посміхатися, танцювати та плакати. Водночас по мірі розвитку програмування та вчинення дій роботами в автономному режимі, постають юридичні питання: чи може аватар бути прирівняний до особи у фізичному світі, особи, яка несе відповідальність та отримує прибуток за дії, вчинені аватаром у автономному режимі. За допомогою та через аватар особа переміщується в репрезентативному просторі віртуальних світів, відшукує нові локації, набуває та створює віртуальні об'єкти, зустрічає інші аватари [616, с. 45].

Ми дотримуємося позиції, що аватар слід віднести до об'єктів прав інтелектуальної власності, який є системою статичних та/або динамічних зображень користувача (реальних чи вигаданих, фантазійних), 2D чи 3D моделей, які можуть містити нікнейм користувача (імена або псевдоніми), що, на думку його автора, є відображенням його особистості у відповідних віртуальних середовищах і є результатом інтелектуальної творчої діяльності автора. Тож таких аватарів у особи може бути декілька, і вони можуть бути різними в залежності від того, в якій ролі постає особа у відносинах віртуального середовища [263, с. 222]. Отож аватар є елементом акаунту та віртуальної ідентичності фізичної особи в інтернеті.

Крім того, в науці та публіцистиці отримало поширення застосування терміна «цифровий двійник». Концепція застосування цифрових двійників була запроваджена НАСА для симуляції при будівництві, випробуваннях та запуску літальних об'єктів. Створення цифрової копії об'єкта стало можливим завдяки розвитку штучного інтелекту, машинного навчання, системи IoT та ін. Цифрові двійники використовуються в аерокосмічній галузі технологій для відстеження руху повітряних суден, точного передбачення погодних умов, виявлення та прогнозування несправності та потреби проведення ремонтних робіт. Наприклад, використання технології цифрових двійників дозволило авіаперевізнику KLM зменшити випадки скасування та невчасного прибуття рейсів [479]. Система цифрових двійників застосовується в технологіях управління життєвим циклом товарів та виробів (Product Lifecycle Management). Система цифрових двійників використовується у проєктуванні будівництва, машинобудування, оптимізуючи витрати в підприємницькій діяльності.

Цифрового двійника можна визначити як програмний аналог фізичного пристрою, який моделює внутрішні процеси, технічні характеристики та поведінку реального об'єкта в умовах навколишнього середовища, для чого використовуються дані з сенсорів (датчиків) фізичного об'єкта, що працює паралельно. Технологія дозволяє проведення порівняння інформації віртуальних датчиків цифрового двійника з датчиками фізичного пристрою, виявлення та встановлення причин відхилень від встановленої мети. Встановлення сенсорів (датчиків) на фізичний об'єкт супроводжується у впровадження на підприємствах технологій промислового IoT [480].

Система цифрових двійників включає двійника з фізичного світу та його цифрову проєкцію у віртуальному середовищі, де представлено один або декілька атрибути двійника з фізичного світу. Концепція цифрового двійника включає створення цифрової проєкції або моделі окремого продукту для підвищення точності обслуговування та прогнозування продуктивності продукту [601, с. 18].

Б. Барікелі, Є. Казірагі зазначають, що характерною особливістю системи є те, що двійники фізичного та цифрового світу пов'язані між собою за допомогою датчиків обміну, які забезпечують синхронізацію між [326]. М.Е. Міллер зазначає, що датчики обміну дозволяють оновлювати дані цифрового двійника по мірі функціонування фізичного об'єкта у своєму середовищі.

Можна назвати такі послідовні елементи, які включає система цифрових двійників: 1) сенсори збирають дані про дії та ефективність фізичного об'єкта в його середовищі, в тому числі дані про становище та зміну умов у фізичному світу; 2) передають зібрані дані від сенсорів (датчики) обміну – цифровому двійнику; 3) проведення аналізу та порівняння, із запланованими змінами в об'єкті; 4) дозволяє прогнозувати (моделювати) майбутню поведінку (становище) фізичного об'єкта у віртуальному середовищі; 5) проєкція майбутньої поведінки порівнюється із поставленою метою; 6) у разі неможливості досягнення поставленої мети, при дотриманні існуючого становища система пропонує варіанти проведення змін у фізичному об'єкті для наближення його становища у відповідність до мети; 7) зміни у цифровій проєкції (двійнику) передаються фізичному об'єкту [668, с. 24].

М.Е. Міллер припускає застосування технологій цифрових двійників не лише для удосконалення функціонування матеріальних об'єктів, а в тому числі у сфері охорони здоров'я для дослідження, профілактики травм, захворювань. Зокрема дослідження ефективності лікарських медикаментів та фармацевтики. На думку науковця, цифровий двійник фізичної особи визначається як інтегрована модель, яка дозволяє передбачати зміни у стані здоров'я фізичної особи з урахуванням навколишнього середовища. Система цифрових двійників людини являє собою фізичну особу та цифрового двійника, який є прототипом людини із її фізичними, фізіологічними властивостями та когнітивними здібностями; де фізична особа та цифровий двійник об'єднані сенсорами (датчиками) таким чином, що зміна властивостей фізичної особи призводить до змін у цифровій проєкції, та навпаки. Функціонування системи цифрових двійників фізичної особи опосередковується технологією IoT. Властивістю

системи цифрового двійника є взаємодія цифрової проєкції у віртуальному просторі та фізичного об'єкта в його звичному середовищі. Зібрані дані, як параметри кісток, м'язів, імітація бігу, ходьбу, інших рухів фізичної особи (аналізи крові, візуалізації, фітнес-датчики тощо), допомагають змоделювати цифрову проєкцію для проведення профілактичних заходів у сфері охорони здоров'я [478].

Тож констатуючи відмінні риси цифрового двійника та цифрового профілю, слід зазначити, що система цифрових двійників дозволяє прогнозувати аварійні ситуації, визначати, які дані необхідні для отримання певного результату, оптимальні способи збору даних та розміщення сенсорів для поставленої мети. Цифровий профіль таких можливостей не має[271, 286].

Отже, поняття цифровий профіль (профайл) людини слід розглядати як різновид узагальнюючого поняття «цифровий профіль (профайл)» або «електронний профайл», який слід розмежовувати на цифровий профіль, який належить людині, та цифровий профіль речей або інтелектуальних агентів.

Слід звернути увагу, що Регламент ЄС 2016/679 передбачає досить широку концепцію персональних даних, так би мовити «плаваючу», коли дані можуть визнаватися персональними даними у разі їх здатності ідентифікувати особу в сукупності з іншими даними. З цього погляду, категорія цифрова ідентичність починає охоплювати досить широке коло персональних даних та категорій. Слід зазначити, що Регламент ЄС 2016/679, будучи нормативно-правовим актом прямої дії, не обмежений територією ЄС та поширюється на всі компанії, які займаються обробкою персональних даних резидентів і громадян ЄС незалежно від того, в якій країні розташована така компанія. Тож якщо українська компанія надає послуги на європейському ринку і працює з персональними даними резидентів ЄС, то вона зобов'язана дотримуватися Регламенту ЄС 2016/679.

На прикладі Instagram можна назвати такі види персональних даних, які компанія зберігає та обробляє при завантаженні світлин користувачів у обліковий запис: 1) вхідні дані та контент, які користувач власноручно створює, як публікації, світлини, коментарі до них, хештеги, публічну інформацію про

профіль тощо. Хоча користувач є правовласником фото за Умовами користувацької угоди Instagram, компанія отримує невиключне та безоплатне право на використання світлин та обробку всіх даних, що містяться на ній; 2) метадані, що містяться на світлині, дані GPS, відомості про камеру, її характеристики та іншу інформацію, що стосуються світлини. Світлина та метадані належать користувачеві, проте Instagram має право використовувати їх; 3) супроводжувальні дані: як фотографія та супутній контент використовуються на платформі, наприклад, кількість лайків, аналітика та коментарі. Такі дані не створюються платформою або окремим користувачем, вони доступні лише компанії Instagram, а фізична особа не має до них доступу, за виключенням користувачів бізнес-акаунтів Instagram; 4) похідні дані, які строюються платформою в результаті аналізу, профілювання вищезазначених категорій, про користувача, наприклад, уподобання, моделі поведінки, інші відомості про користувача. Такі дані, будучи цінними для компанії, використовуються для удосконалення, розробки та дослідження продуктів компанії, маркетингової стратегії, до яких користувачі зазвичай не мають доступу [131].

Слід зазначити, що компанії також збирають та обробляють такі дані як стан фізичної активності, що відстежується смарт-годинками та іншими пристроями, дані про маршрути, завантаження дорожньо-транспортної структури, що збирається транспортними засобами. Постає слушне питання, чи можуть ці дані бути охоплені категорією «цифрова ідентичність».

Відповідно до ч. 5 ст. 4 Регламенту ЄС 2016/679 в разі застосування псевдоанімізації персональних даних, прийняття технічних заходів, які запобігають співвіднесенню інформації з фізичною особою, унеможливлюється ідентифікація конкретного суб'єкта без використання додаткової інформації за умови, що така інформація зберігається окремо. Тобто в разі застосування псевдоанімізації запобігається віднесення даних до ідентифікованої або підлягаючої ідентифікації фізичної особи. Персональні дані будучи анонімізованими, псевдоанімізованими стають індустріальними або промисловими даними. Такі дані бувши відділеними від фізичної особи, за

визначенням К.Г. Некіт, являють інтерес для компаній, які розроблять програмне забезпечення держаних установ (для підвищення рівня якості сервісів та ситуації на дорогах), відносяться до промислових або індустріальних даних. Індустріальні дані зазвичай відображають функціональність систем, пристроїв, агрегатів, вочевидь мають відмежовуватися за правовим режимом та відрізнятися від персональних даних [116, с. 57]. Тож анонімізовані, псевдоанімізовані дані не дозволяють ідентифікувати фізичну особу та не охоплюються категорією «цифрова ідентичність».

Враховуючи викладені думки, можна зазначити, що цифрова ідентичність фізичної особи в інтернеті розуміється у двох значеннях: у широкому та вузькому. Цифрова ідентичність у вузькому значенні розуміється як віртуальний образ суб'єкта цивільних відносин – акаунт, який створюється внаслідок активних дій фізичної особи для певної мети та складає систему даних (джерело персональних даних особи та її прав і обов'язків) про фізичну особу, в певній інформаційно-комунікаційній системі, які ідентифікують її у відповідних системах (органів держаної влади та місцевого самоврядування, фінансових установ та організацій, у соціальних мережах тощо), дані можуть автоматично оновлюватися під час їх зміни в інформаційних системах державних органів та установ. У вузькому значенні цифрова ідентичність створюється в результаті активної діяльності особи для досягнення певної мети. Наприклад, на різних платформах та соціальних мережах фізична особа може по-різному себе позиціонувати. У вузькому значенні цифрова ідентичність збігається із визначенням акаунту.

У широкому значенні цифрова ідентичність розуміється як система усіх даних про фізичну особу в цифровому середовищі (сукупності психологічних, емоційних, фізичних, соціальних властивостей особи) без прив'язки до конкретного акаунту, включаючи дані, які особа залишає в результаті як активної, так і пасивної діяльності, яка не спрямована безпосередньо на розкриття даних. Означений підхід до цифрової ідентичності у вузькому та широкому значенні отримав правове закріплення у французькому законодавстві

в галузу спадкування та встановлення доступу до цифрової спадщини після смерті фізичної особи.

Елементами цифрової ідентичності в широкому значенні можна назвати: акаунти, персональні дані, цифрові сліди та результати діяльності фізичної особи у вигляді публікацій, дописів, світлин, лайків та інших даних, за виключенням анонімізованих персональних даних або псевдоанімізованих даних, обробка яких відбувається способом, який не дозволяє їх віднести до конкретної особи без використання додаткової інформації та конкретно ідентифікувати її.

Користувачі соціальних мереж можуть обмежувати доступ до даних акаунту, обмежуючи та закриваючи його для перегляду решти користувачів. Водночас персональні дані, які формують профіль фізичної особи, її інтереси та уподобання, як закритого та відритого акаунту, однаково збираються, обробляються цифровими майданчиками та соціальними мережами.

Слід зазначити, що визначення цифрової ідентичності як у вузькому, так і широкому розумінні має не лише доктринальну роль, а й практичну юридичну значущість як соціального явища. Такий підхід актуалізує проблему визначення обсягу розпорядження особою (облікові записи, цифрові гроші, об’єкти інтелектуальної власності, цифрові речі та ін.) на випадок смерті, та виявити складнощі реалізації широкого підходу на практиці в мережі «Інтернет». Норми французького права враховують як вузький, так і широкий підхід до розуміння цифрової ідентичності, пропонуючи рішення до проблеми цифрової смерті. Так, Закон Франції про захист даних і свободи від 17.12.2015 доповнено ст. 40-1[631], деталізує порядок розпорядження даними особи після її смерті. Особа може залишити відповідні розпорядження на випадок смерті, які поділяються на загальні, що встановлюють волю особи про використання всієї сукупності даних про неї, і спеціальні, що встановлюють волю особи на розпорядження конкретними акаунтами та персональними даними. Даний приклад свідчить, що реалізація широкого підходу до цифрової ідентичності може актуалізувати складні питання на випадок смерті користувача, пов’язані з необхідністю пошуку всіє сукупності сервісів, які використовувала особа, а частина сервісів

або акаунтів можуть забуватися користувачем ще за життя. За відсутності можливості визначити всі сервіси досить складно встановити коло відповідальних осіб у частині видалення інформації користувача або передання цих даних спадкоємцям.

Відтак право на цифрову ідентичність (у вузькому та в широкому розумінні) у приватних інформаційних системах має розумітися як право фізичної особи на цифрову ідентичність – персональні дані, створювані нею акаунти та інші дані в мережі. Помітною є різниця у визначенні акцентів, якщо у випадку цифрової ідентичності у вузькому сенсі – вирішальне значення приділяється зв'язку між метою створення цифрової ідентичності та її змістом, то у випадку цифрової ідентичності в широкому сенсі – вирішальне значення має обсяг даних, який залишається цілеспрямовано або випадково. Тому цифрову ідентичність у науці пропонують розуміти як інформацію, яка безпосередньо розкривається фізичною особою з певною метою при створенні акаунту, або як системи всіх даних, які свідомо або випадково залишає фізична особа в інтернеті.

Серед властивостей цифрової ідентичності називаються такі як: можливість анонімно вступати у відносини з третіми особами, під якою розуміється можливість приховування дійсного імені в межах дозволених законодавством; можливість ідентифікації та наділення особи необмеженою низкою ідентифікуючих ознак; множинність – можливість володіти низкою цифрових ідентичностей у межах дозволених законодавством (в іграх); автоматизація – можливість повністю або частково симулювати активність цифрової особи з використанням комп'ютерної програми (пов'язує з робототехнікою) [829, с. 281].

Слід також звернути увагу на таку властивість цифрової ідентичності як її похідний характер від «творця» – фізичної особи. Значущість даної властивості обумовлена виникаючими питаннями у науці: чи володіє цифрова ідентичність здатністю до прояву волі та волевиявлення, чи володіє цифрова ідентичність автономною волею (як прояву незалежності від зовнішніх впливів, як здатність до управління)[125]. У загальновживаному значенні Н.А. Мяловицька розуміє

під автономією відокремленість, самостійність, незалежність (наприклад, автономія розуму, автономія прав, автономія волі тощо) [111, с. 93].

В «Юридичній енциклопедії» автономія визначається як відносна самостійність у здійсненні влади [284, с. 23]. Особиста автономія у правовому розумінні є не стільки проявом людської психології, скільки продуктом юридичного конструювання (зокрема, самовизначення) правової індивідуальності особи, її юридичної персональності або правосуб'єктності [276, с. 54].

Ю.В. Шеляженко називає такі ознаки особистої автономії приватних осіб та організацій, які можуть застосовуватися на практиці при вирішенні питання визнання за об'єктом права, статусу особи (суб'єкта права): індивідуальне самовизначення (ідентичність); самостійність існування за власними законами в силу автономії матерії, автономії волі, суверенітету розуму; здатність бути першоджерелом власного невідчужуваного права; здійснення суб'єктивних прав і обов'язків; свобода вибору правових засобів здійснення правомірних інтересів; проявлена у правових процесах і відносинах здатність розвивати свободу на основі правового досвіду відповідальності [276, с. 54].

О.В. Грищук, Х.Т. Слюсарчук серед основоположних цінностей лібералізму називають свободу особистості, яка випливає з принципу індивідуалізму і прагнення забезпечити кожному індивіду можливість діяти на власний розсуд [47, с. 27].

Автономія особи є важливим принципом у практиці ЄСПЛ, який обґрунтовує розуміння гарантій, передбачених правом на повагу до приватного та сімейного життя самостійним правом, що випливає з поняття «особисте життя», доповненим правом на особистий розвиток та можливістю, що передбачає ефективне здійснення пов'язаних з нею прав.

Для того, щоб бути носієм прав та обов'язків, особі необхідно володіти зовнішньою відособленістю; здатністю до вираження та здійснення власної волі [270, с. 45]. Саме здатність до вираження автономної волі може бути передумовою правосуб'єктності особи. Здатність формувати та реалізовувати

самостійно та відокремлено власну волю характеризує суб'єкта як учасника цивільних правовідносин.

З урахуванням зазначеного, цифрова ідентичність фізичної особи не володіє: зовнішньою відособленістю, автономією або свободою; здатністю виражати та здійснювати персоніфіковану волю, відмінну від фізичної особи. Цифрова ідентичність не володіє здатністю до самостійної участі у цивільних відносинах автономно від фізичної особи; вона перебуває в залежності від фізичної особи і їй не властива здатність до володіння волею автономно від фізичної особи; власними правами та обов'язків, які є окремими від фізичної особи. Цифрова ідентичність не має реальної здатності своїми вольовими фактичними діями самостійно здійснювати права та виконувати обов'язки, а є похідною від її «творця», будучи його продовженням виражає волю фізичної особи. Тому на противагу фізичній особі, яка володіє свободою, цифрова ідентичність не володіє автономною волею від фізичної особи, не виступає як автономний учасник цивільно-правових відносин та виражає волю фізичної особи.

Підсумовуючи викладені позиції, можна назвати такі властивості цифрової ідентичності у вузькому розумінні: репрезентативність – представляє суб'єкта цивільних відносин (цифровий образ); нематеріальність – є джерелом персональних даних у мережі, які не підлягають зношенню та амортизації; транскордонність – можливість здійснення прав та обов'язків без прив'язки до традиційних кордонів держав; економічна цінність – елементи цифрової ідентичності можуть характеризуватися попитом та пропозицію, відчужуватися та приносити економічну вигоду її власнику; створюється в результаті активних дій фізичної особи для певної мети та складають набір даних про фізичну особу, в певній інформаційно- комунікаційній системі, які ідентифікують її у відповідних системах (органів держаної влади та місцевого самоврядування, фінансових установ та організацій, у соціальних мережах тощо), дані можуть автоматично оновлюватися під час їх зміни в інформаційних системах державних органів та установ; залежність та похідний характер від її «творця»

фізичної особи (виражає її волю, не виражає власну автономну волю; перебуває в залежності від фізичної особи та не володіє реальною здатністю своїми вольовими фактичними діями самостійно здійснювати цивільні права та виконувати обов'язки); проєктність або множинність цифрової ідентичності обумовлена відносною анонімністю персональних даних для широкого загалу користувачів (постачальники телекомунікаційних послуг отримують доступ до персональних даних користувачів, які можуть бути передані уповноваженим органам).

Поряд із категорією цифрова ідентичність, набуває використання такий термін як «децентралізована ідентичність» або «суверенна ідентичність». В умовах підвищення ризиків витоку персональних даних, високих штрафних санкцій у разі порушення законодавства, значно зросли вимоги до контролерів даних Регламентом ЄС 2016/679 та Законом Каліфорнії Про конфіденційність споживачів від 2018 року. Законодавство передбачає вимоги належного здійснення таких прав користувачів як: право на доступ до персональних даних; право знати, які дані збирають компанії про користувачів; право бути забутим; право на видалення; право на перенесення даних тощо [362]. Означене та розвиток технології, орієнтованої на користувачів на платформі блокчейн та розподільних реєстрів, стали поштовхом для концепції «децентралізованої цифрової ідентичності» [464], «суверенної цифрової ідентичності»[465], яка покликана забезпечити управління, контроль за доступом за персональною інформацією, чутливими персональними даними децентралізовано, тобто без участі третьої сторони, постачальника ідентифікаційних даних, центру сертифікації або розпорядника реєстру.

На відміну від «централізованої ідентичності», умови якої передбачають володіння та управління персональними даними централізованими органами та організаціями, що несе високий ризик витоку даних; збір, обробка та передача персональних даних без відома особи, забезпечує: володіння та контроль за персональними даними та їх передачу за згодою фізичної особи; централізоване зберігання в «гаманцях» користувачів, що знижує ризики масових витоків даних

та порушень[789]. У свою чергу, концепція децентралізованої або суверенної цифрової ідентичності, як припускається, покликана повернути користувачам контроль над цифровою ідентичністю за допомогою профайлу, в якому акумулюються дані про фізичну особу від уповноважених органів.

Існує твердження, що концепція суверенної ідентичності виникла внаслідок спроби реалізувати Вестфальську систему міжнародних відносин, яка виникла в Європі на основі угоди про Вестфальський мир, внаслідок тридцятирічної війни, що закінчилася у 1648 році [31].

Традиційно термін «суверенітет» значний час використовується по відношенню до державного суверенітету[206, с. 48]. За визначенням Кембриджського тлумачного словника, суверенітет розуміється як володіння найвищою владою та правом бути повністю незалежним [800].

Наразі термін «суверенітет» використовується в роботах сучасних соціологів, політологів, філософів по відношенню до суверенітету особи. Водночас визнання та забезпечення суверенітету особи як однієї з головних засад існування суспільства відбувалося ще в римському приватному праві [264, с. 10]. За визначенням Є.Л. Стрельцова, суверенітет особи, з одного боку, є об’єктивною мірою її незалежності від держави і суспільства, а з іншого – характер і форми її взаємовідносин із ним.

Відповідно до ідеї розробників концепції суверенної ідентичності в мережі «Інтернет», можливість незалежного (суверенного) самоврядування є «вродженою» властивістю людини, а проведення реєстрації забезпечує участь у правових відносинах. Акт реєстрації передбачає, що для існування цифрової ідентичності необхідний контрольований суспільством процес адміністрування.

Під концепцією цифрової суверенності ідентичності розуміється здатність фізичної особи вчиняти дії та ухвалювати рішення у свідомий і незалежний спосіб, володіння найвищим контролем над власними персональними даними, програмами та іншими технологіями, можливість управління своїми персональними даними та цифровою ідентичністю.

Особливістю технології, орієнтованої на користувачів, суверенною ідентичністю є збереження за фізичною особою контрольної копії персональних даних у хмарі в папках Dropbox, Google drive або цифровому гаманці. Кожна така хмара з персональними даними підтримується програмним забезпеченням, яке допомагає користувачеві впорядковано зберігати дані, мати доступ до них та надавати доступ третім особам до певних фрагментів цих даних.

Концепція суверенної ідентичності засновується на: децентралізованій базі даних, які спільно використовується на комп'ютерах, об'єднаних мережею на платформі блокчейн, що записують та зберігають дані, ускладнюючи можливість зміни, зламу та витоку даних; криптографічному захисті облікових даних, які особи надають на вимогу організацій для верифікації; криптографічно перевірених ідентифікаторах (персональних даних) створюваних користувачем, які йому належать та не залежать від установ [465].

Усі дані, що зберігаються у хмарі персональних даних, можуть поповнюватися з різних джерел: додаватися фізичною особою шляхом завантаження копій документів; або можуть бути агреговані у хмару даних від сторонніх агрегаторів або процесорів даних автоматизовано, за допомогою програми, яка забезпечує функціонування хмарного сховища. Отримання персональних даних від сторонніх постачальників послуг в ЄС передбачено ст. 15(3) Регламенту ЄС 2016/679 «право на отримання копії даних» та ст. 20 Регламенту ЄС 2016/679 «право на перенесення даних». Право на перенесення персональних даних передбачено також ст. 1798.110 та S. 999.312 Закону Каліфорнії про захист персональних даних [814].

Модель даних, що зберігаються в користувача, має такі важливі наслідки. По-перше, маючи можливість зберігати персональні дані у хмарі, користувач може краще розуміти масштаби даних, що збираються, обробляються відносно нього. По-друге, модель дозволяє відокремити дані користувача від програм: в екосистемі даних користувача програми працюють, так би мовити, «поверх» будь-яких даних, що зберігаються у хмарі персональних даних. Це відображає ідею права на перенесення даних, передбачену ст. 20 Регламента ЄС 2016/679:

після отримання даних від обробника даних та їх зберігання у хмарі персональних даних ці дані більше не повинні «мандрувати» до іншого постачальника послуг; натомість постачальник послуг може отримати доступ до персональних даних користувача лише за його попередньою явно вираженою згодою та на умовах, що визначаються ним самим. Людина може здійснювати такий контроль шляхом надання дозволу доступу до даних: дозволи на доступ до даних можуть мати безліч рівнів (наприклад, доступ на певний період часу, для певної мети/функції та для конкретної третьої сторони). Оскільки сторонні програми встановлюються поверх даних користувача, ці програми можуть за замовчуванням отримати доступ тільки до того сегменту персональних даних людини, який необхідний для виконання конкретної функції програми.

З точки зору контролера або постачальника послуг, пропозиція послуг з обробки даних у хмарі персональних даних користувача не лише виступає певною гарантією законності використання даних, а також надає можливість отримувати послуги в умовах та компаніям, які дотримаються вимог п. a, b, c. ч. 1 ст. Регламенту ЄС 2016/679. Так, доступ до даних безпосередньо від окремої особи відповідає принципам мінімізації даних, оскільки постачальник послуг не зобов'язаний зберігати будь-які дані на власних серверах. Дотримується принцип обмеження мети, оскільки персональні дані використовуються лише для конкретної мети, на яку користувач надав попередню згоду.

Слід припустити, що модель суверенної або децентралізованої цифрової ідентичності знижує ризики масових витоків та порушень, обумовлених збором, зберіганням, обробкою персональних даних на серверах контролерів та надає фізичній особі більше важелів контролю, володіння за його персональними даними, а з тим і права власності на персональні дані.

У науці висловлюється дискусійне питання доцільності визнання права власності на персональні дані або права власності на цифрову ідентичність.

С. Кроуфорд висловлює стурбованість, що онлайн-посередники (компанії, які створюють онлайн-середовище, наразі ігри, але в майбутньому, світи, які можуть стати новим інтернетом) впроваджують норми та правила, які наділяють

їх правом «власності» на цифрову ідентичність та можливість вирішення долі щодо її видалення [445, с. 7]. Науковець навіть висуває тезу про те, що посередники є непідзвітними, а правила, які вони встановлюють, неможливо оскаржити в суді, наділяючи їх повноваженням до правотворчості. Науковець замислюється над питанням власності на цифрову ідентичність та на цифрову репутацію.

Тож із питанням прав на цифрову ідентичність пов'язується питання визнання права на персональні дані фізичної особи в мережі «Інтернет», що є предметом наукових дискусій.

К. Тротьє дотримується позиції, що саме корпорації, не держава, отримують прибутки від використання зібраних персональних даних, проте єдиними власниками цифрових ідентичностей мають залишатися користувачі, що має забезпечуватися належними гарантіями захисту. Науковець критикує ситуацію, за якою приватні корпорації набувають права на персональні дані [831].

П. Джеркус стверджує, що технології, засновані на моделі даних, «орієнтованих на користувача», дозволяють особам збирати, керувати та володіти персональними даними в одному місці та зберігати копії своїх даних у «хмарах персональних даних» (аналогічно Dropbox, який дозволяє зберігати дані користувачів). Кожна хмара персональних даних підтримується програмним забезпеченням, яке надає можливість керування ними [588]. Науковець дотримується позиції визнання права власності користувачів на персональні дані.

П. Джеркус зазначає, що користувальницькі персональні дані є найточнішою та актуальною інформацією про фізичну особу, які відповідають усім вимогам, що пред'являються до активів у законодавстві про право власність, незважаючи на те, що вони є нематеріальними. Економічні переваги застосування режиму права власності на персональні дані має надати переважні можливості суб'єктам даних у здійсненні їх прав, та стати гарантією захисту від порушень з боку третіх осіб, постачальників послуг, які зберігають персональні

дані та отримують від них переваги. Науковець наполягає, що концепція права власності на персональні дані відповідає положенням, передбаченим Регламентом ЄС 2016/679 та Законом Каліфорнії Про конфіденційність споживачів від 2018 року. За ствердженням П. Джеркуса, визнання прав власності має стати необхідною передумовою для створення нової системи обробки даних, в якій дані відокремлені від додатків, а програмне забезпечення функціонує, так би мовити, «поверх» персональних даних користувачів [589, с. 5].

Погляди на користь визнання права власності на персональні дані набули поширення через скандали, обумовлені політичними перегонами Д. Трампа та BREXIT. Так, колишня співробітниця компанії Cambridge Analytica, Б. Кайзер заснувала громадську організацію, яка підіймає обізнаність суспільства та просуває ідеї визнання персональних даних об'єктами права власності [364]. Правозахисниця у своїх виступах наголошує на необхідності забезпечення балансу приватних та публічних інтересів для ефективного розвитку охорони здоров'я та винайденню нових лікарських медикаментів, проведення досліджень та випробувань, що вимагає збір та обробку персональних даних. Водночас суб'єкти даних мають право знати мету, цілі обробки даних тощо [364]. Наразі визнання персональних даних об'єктами права власності, яке б давало фізичним особам право власності над своїми персональними даними, ще не отримало прямого правового закріплення в законодавстві, хоча визнається за персональними даними їх мінова властивість. Як слушно зазначає Н.Ю. Голубєва, персональні дані вже давно стали «Інтернет-валютою» [43, с. 4]. Обґрунтовують позицію доцільності визнання персональних даних об'єктами права власності: К.Г. Некіт [116, с. 57], П. Джеркус [588], Дж. Ріттер, А. Маєр [773, с. 220]. Як зазначають, Є.О. Харитонов, О.І. Харитонова[265, с. 5], що данні особи, які складають цифрову особистість за її життя, якщо не відбулося втрати тілесності, належать самій людині після її смерті – правонаступникам у вигляді цифрової спадщини.

Означений підхід ґрунтується на обставині, що платформи використовують персональні дані з комерційною метою, що припускає можливість визнання мінової цінності за персональними даними, які надаються користувачем. Як свідчать соціологічні опитування, закріплення можливості за користувачами здійснення контролю за даними сприяло б створенню середовища довіри між користувачами та платформами [745, с. 22]. Надані дані можуть отримати певний грошовий вираз залежно від того, наскільки вони є корисними. Адже будь-яка послуга в мережі «Інтернет» як платна, так і безоплатна, надається за певну зустрічну дію – надання персональних даних користувачем. Тому висувається теза про надання особам права обирати чи розраховуватися грошовими коштами, чи персональними даними за послуги в мережі.

Поряд із вищевикладеною позицією, в юридичній літературі існує підхід, що заперечує ідею виключного права власності на персональні дані. Серед противників можна назвати Дж. Дрексла [482], який стверджує, що не існує концепції, яка б обґрунтувала право власності на персональні дані.

С. Делакруа піддає критиці право власності на персональні дані, надалі пропонує концепцію трасту даних, який може працювати та функціонувати лише в разі, якщо засновник є власником трастових активів. Науковець також наполягає на відмові від концепції права власності на персональні дані фізичної особи, застерігаючи, що таке твердження не виключає права власності на компанію, що збирає та обробляє персональні дані [470, с. 6].

Дж. Дрексл вважає, що не існує принципу або теорії, які виправдовували б виокремлення виключних прав власності на дані та стверджує, що будь-яке визнання нового права власності, наприклад, права власності на (персональні чи неперсональні) дані, потребуватиме додаткового обґрунтування[483]. Причина такої позиції також обґрунтовується в науці досить широкою концепцією персональних даних відповідно до Регламенту ЄС 2016/67, яка вимагає від контролерів оцінювання чи може інформація безпосередньо або опосередковано ідентифікувати особу в сукупності з іншими даними [773, с. 220].

Французька дослідниця Л. Мерзо відходить від ідеї цифрової ідентичності на користь «присутності в мережі», звертає увагу на цифровий слід, який особа залишає поза своєю волею, та пропонує говорити про контроль за даними, які суб'єкт залишає під час використання в мережі «Інтернет», у тому числі право контролювати використання історії вчинків [674, с. 33].

Опоненти визнання права власності на персональні дані стверджують [588; 589 с. 8], що передбачений у законодавстві ЄС підхід базується на правовому регулюванні саме «доступу» до персональних даних, який відображений в Європейській стратегії для даних 2020 [495] та Білій книзі ЄС про ШІ [849]. Означений підхід базується на ідеї права доступу та управління цифровою ідентичністю. Крім того, також спостерігається тенденція закріплення права на здійснення контролю за персональними даними та закріплення права на перенесення даних у Регламенті ЄС 2016/679.

За ст. 15 Регламенту ЄС 2016/679 передбачається саме право доступу до персональних даних, яке дозволяє здійснювати інші права суб'єктів даних як право виправлення первинних даних та результатів профілювання, прав на видалення, право на отримання компенсації за збитки та звернення до третіх осіб, отримувачів персональних даних, у разі їх передання контролером. На користь «доступу» до даних свідчить також ч. ст. 15 Регламенту ЄС 2016/679, яка передбачає обов'язок контролера надати саме копію персональних даних, які обробляються.

Крім того, варто зазначити, що технології обробки даних удосконалюються та розробляється технологія децентралізованої моделі управління даними із застосування технології блокчейн, яка дозволяє здійснювати основну обробку даних у хмарі.

Означені твердження підкріплюються розвитком технологій Web 3 на платформі блокчейн та розподільних реєстрів, які сприяють розробці технології децентралізованої цифрової ідентичності, яка має надати право доступу до єдиної цифрової ідентичності, право контролювати доступ до даних та забезпечити право переносити дані з однієї платформи на іншу [585]. Разом з

цим, слід взяти до уваги, що цифрова ідентичність (у широкому розумінні) формується не лише в інформаційних системах приватних компаній, а й внаслідок збору та обробки персональних даних, профілювання, соціального рейтингу та автоматизованої обробки, збору даних з камер віддаленої біометричної ідентифікації, акаунтів (профайлів) в інформаційних системах державних та правоохоронних органів, акаунтів у державних системах охорони здоров'я, які являють публічний інтерес.

З урахуванням викладеного, можна говорити про право на цифрову ідентичність, як особисте немайнове право, обумовлене розвитком технологій, яке належить кожній фізичній особі, є комплексним за своєю структурою і складається з права на визнання цифрової ідентичності, право перешкоджати будь-якому спотворенню та посяганню на цифрову ідентичність, яке може завдати шкоди фізичній особі.

Підсумовуючи вищевикладене, слід зазначити, що в сучасних умовах акаунти в соціальних мережах, електрона пошта із активним профілем, реєстрація на сайтах для отримання доступу є невід'ємною складовою користування всіма благами сучасного цифрового суспільства, невідворотним стає формування категорії цифрової ідентичності фізичної особи в мережі «Інтернет». Сучасний розвиток та поширення використання інформаційних технологій у суспільстві дозволяє говорити про цифрову ідентичність як систему даних про особу, представлену в цифровій формі, з використанням якої особа вступає у правовідносини, здійснює права та набуває обов'язки в мережі. Така цифрова ідентичність представляє та діє завдяки фізичній особі.

2.2. Формування концепції цифрової ідентичності фізичної особи в мережі «Інтернет»

Формування конвергентного віртуального середовища із образом життя, відмінного від фізичного світу, трансформує місце та властивості фізичної особи. Завдяки поширенню інформаційних технологій та інтернету відбувається взаємопроникнення віртуального світу та фізичної реальності, стирання меж між категоріями реального та віртуального світів, висування на перший план не реальної людини, а електронного профайлу людини або віртуального образу в мережі «Інтернет». Висувається навіть позиція, що користуючись інтернетом, фізичні особи створюють власну цифрову копію, яка здійснює її права та обов'язки у віртуальному середовищі [87].

Цифровізація впливає на потребу осмислення усталених наукових підходів з урахуванням впливу цифрового середовища з його специфічними властивостями, які зумовлюють появу дискусій щодо суб'єкта права, його прав та обов'язків у цифровому середовищі та навіть висувають тезу про появу принципово нових суб'єктів права.

Роздуми про особистість і способи її ідентифікації за допомогою технології блокчейн висувають ідею цифрової особистості як системи даних, псевдонімів, які використовуються для взаємодії в інтернеті. У сфері ідентифікації відбувається прив'язка фізичної особи до цифрової ідентичності.

Кожного разу авторизуючись на платформах, користувачі використовують віртуальну ідентичність, яка їх презентує навіть у період відсутності [843].

Розглядаючи зміст поняття цифрової ідентичності як однієї з базових категорій у цифровому середовищі, слід зазначити, що термін «ідентичність» походить від латинського кореня idem, що означає «такий самий», тобто позначає властивість або тотожність осіб, персональних або індивідуальних властивостей [774, с. 25]. Термін «ідентичність» також використовується для позначення стану або факту тотожності, однаковості, співпадіння окремих аспектів [577]. Те, що у фільмі «Матриця» названо «ментальною проєкцією

віртуального Я», по суті є образом ідентичності – тим, якою людина звикла себе сприймати та бачити.

Сучасні технології та мережі забезпечують певний рівень анонімності, що мотивує для створення віртуальної ідентичності, яка безпосередньо нетотожна користувачу. Завдяки анонімності виникає можливість трансформації та маніпулювання властивостями особи, наділення користувачів правом представляти різні версії себе в мережі. У такий спосіб, штучно створюючи віртуальну проєкцію особи, яка демонструє якості та властивості, яких позбавлена референтна особа користувача.

У філософії зазначається, що технології розширили можливості вираження ідентичності, наділення новими властивостями, які не співпадають із характеристиками особи у фізичному світі [214, с. 292].

Соціальні мережі створили можливості не лише для вільного вираження творчості, а й експериментів із ідентичністю, дозволили репрезентувати вигаданих осіб, приміряти різні ролі, маски та ідентичності, що складно реалізувати у фізичному світі [498, с. 311].

Створення фіктивної віртуальної ідентичності може бути мотивоване засадами конфіденційності, безпеки, крім того, віртуальна особа може бути видалена безслідно[341]. В інтернеті створення симулякрів переважно обумовлюється розважальною складовою [237, с. 47].

Ф. Джеймсон називає суб’єкта, перебуваючого у процесі ідентифікації – «тілом» або поверхнею, що відображає його соціальні та культурні взаємозв’язки [580, с. 48]. На думку В. Ходжсон, ідентичність, створюється особою під час комунікації, вираження та позиціонування в мережі [561, с. 229].

На погляд Я. Коксвіка, віртуальна ідентичність є не новим явищем, оскільки можливість використовувати псевдоніми для збереження анонімності існувало й до появи інтернету. Провідна відмінність із минулими періодами історії полягає у функціонуванні автоматизованих систем та інтелектуальних агентів [842, с. 77].

Наразі психологи наголошують, що у фізичному світі феномен альтернативної ідентичності є свідченням психологічного відхилення. М. Бек та Р. Уілсон заперечують побудову альтернативної ідентичності, адже психологічно здорова особа прагне до тотожної автентичності та самоактуалізації як у реальному житті, так і у віртуальному середовищі. Електронні інструменти само презентації, такі як аватари та нікнейми, сторінки в соціальних мережах дають змогу користувачам вільно конструювати символи, що відображають їх реальну ідентичність [320, с. 372; 871, с. 203].

Спеціаліст у галузі комп'ютерної комунікації Ш. Теркл описує інтернет як середовище для вирішення та розв'язання психологічних конфліктів із використанням нових інструментів кіберпростору [838, с. 643].

М. Кастельс [418, с. 240] та Дж. Сулер [806, с. 455] наголошують, що уявна анонімність в інтернеті створює передумови для зловживання правом та прояву девіантної поведінки осіб.

На думку В.Н. Мортеза, анонімність сприяє вчиненню правопорушень в інтернеті. У мережі «Інтернет» існують перепони в ідентифікації порушника обумовлені анонімністю [675, с. 5]. На відміну від реального світу, де закон може обмежувати свободу вибору та вираження, в кіберпросторі користувачі володіють правом вільного вираження [551].

У цифровому середовищі уявна свобода від обмежень та правил, властивих фізичному світу, де дотримання правових норм забезпечується державними примусом, підштовхує до вчинення правопорушень. Дж. Грохол зазначає, що віртуальне середовище, завдяки анонімності, несе виклики, які змінюють властивості ідентичності [545].

У 90 роках існував афоризм, що стосувався карикатури в журналі «Нью-Йоркер»: «В інтернеті ніхто не знає, що ви собака» [779, с. 557].

Слід визнати, що на первісних етапах розвитку інтернету законодавство не обмежувало у вільному виборі ідентифікуючих ознак особи, свобода існувала без обмежень в інтернеті. Особа могла вільно презентувати, обирати, змінювати власні характеристики та ознаки [551, с. 71]. Провідними рисами ідентичності

на первісному етапі розвитку інтернету у 1970-1990 були: анонімність, множинність цифрової ідентичності та можливість контролювати з боку фізичної особи. Подібні погляди спиралися на особливості програмної архітектуру первісних мереж, які забезпечували певний рівень анонімності. Серед властивостей цифрової ідентичності називалась можливість надання недостовірних даних про себе, суб'єкти правовідносин в інтернеті могли залишатися неідентифікованими, оскільки технічні засоби ідентифікації не могли однозначно ідентифікувати суб'єкта, створюючи юридичну фікцію або презумпцію певної особи. Інтернет створював уявлення простору безмежних можливостей, анонімного спілкування та вільного самовираження, яке забезпечує високий рівень недоторканності приватного життя в цифровому середовищі, де під маскою анонімності може ховатися будь-яка особа, а поведінка жодним чином не контролюється та не фіксується.

На даних етапах розвитку інтернет заповнювався контентом, створеним науковцями, інженерами, які дотримувалися принципу свободи інформації. Інтернет розглядався як суспільний електронний ресурс, простір безмежних можливостей для самоідентифікації та приватності. Технологія інтернету, будучи створеною для задоволення потреб та інтересів оборонної промисловості, характеризувалася анонімністю, відсутністю правового регулювання, та лише по мірі розвитку технологій стала загальнодоступною для всього суспільства.

Розробка технології інтернету в перші роки описувалася прибічниками ліберального підходу правового регулювання мережі, як глобальний простір, в якому обмін думками та поглядами відбувається вільно, незалежно від державних кордонів та анонімно.

Одним із ключових постулатів на первісному етапі розвитку інтернету та віртуальної реальності називалось анонімне спілкування та вільне самовираження, яке припускало широкий обсяг права на недоторканність приватного життя в цифровому середовищі. Визнавалась надзвичайна привабливість анонімності, яка була притаманна відносинам в інтернеті на первісних етапах його розвитку [333].

Користувачі були наділені правом вільного вибору та зміни масок, зміни ідентичності, псевдонімів, під якими вони себе презентували, що створювало ілюзію анонімності в мережі. Користувачі мали право вирішувати, чи розкривати своє справжнє ім'я, чи використовувати вигадане (нікнейм, псевдонім).

На означеному етапі був сформований та розвинений принцип мережевого нейтралітету [683] для захисту світового інформаційного простору від будь-яких обмежень та правового регулювання з боку провайдерів, державних органів; користування контентом, вибору доменних імен, свободу доступу до інтернету тощо.

Визнаючи значущість мережевого нейтралітету, притаманного інтернету від початку, необхідно визнати зміни, які відбулися з того часу, еволюцію суспільства та інформаційно-комунікаційних технологій. Анонімність стала провокаційним чинником вчинення порушень та девіантної поведінки в мережі [757, с. 16]. Наразі інтернет-середовище характеризується девальвацією анонімності, конфіденційності та не відрізняється від будь-якого публічного офлайн-простору, де можуть вчинятися правопорушення.

На сучасному етапі розвитку мережі «Інтернет» не можна погодитися з позицією, що особа володіє безмежною свободою, вільним вибором ідентичностей. Сучасний інтернет характеризується відсутністю абсолютної анонімності; вимогами ідентифікації суб'єктів правовідносин у мережі, цифрова автентифікація є умовою укладання правочинів в інтернеті; в разі вчинення правопорушення в мережі, особа буде притягнена до відповідальності у фізичному світі.

Наразі нагальними є питання, пов'язані з анонімністю, у зв'язку з потребою в ідентифікації користувачів у мережі «Інтернет» як учасників цивільних правовідносин, здійснення правосуб'єктності осіб та захистом основних прав та свобод людини. З одного боку, держави, в рамках своїх міжнародних зобов'язань щодо захисту прав і законних інтересів осіб, поступово запроваджують правове регулювання за інтернет-середовищем, запроваджуючи заходи з ідентифікації користувачів. З іншого боку, GAFAM обмежують засади

анонімності у правилах користування платформами, просувають політику єдиної автентичної ідентичності, реальних імен, зацікавлені в отриманні достовірної та якомога повної інформації про користувачів, з метою індивідуалізації послуг та реклами.

Висловлюється думка, що анонімність є гарантією здійснення таких фундаментальних прав людини в мережі як недоторканність приватного життя та права на таємне листування тощо [776, с. 65; 779, с. 557]. Проте, якщо на первісних етапах анонімність вважалася однією із ключових ознак інтернету, а програмна архітектура не передбачала передання даних про користувачів до кінцевого обладнання, то сучасний інтернет характеризується протоколом відкритого, а не конфіденційного спілкування, де анонімність ілюзорна. Властивістю сучасного інтернету є те, що навіть приховуючись під вигаданими ідентифікаційними даними, користувач залишає після кожної дії в інтернеті «цифрові сліди» (пошукові запити, відвідування сторінок), аналогічно залишеним у фізичному світ, які можуть сприяти ідентифікації реальної фізичної особи, представленої цифровою ідентичністю. Зокрема сприяти ідентифікації особи можуть цифрові сліди в поєднанні з технічними даними (дані про девайс, оператора зв’язку, динамічна або статична IP-адреса, місцезнаходження пристрою тощо) та індивідуальними даними, про властивості взаємодії користувача із пристроями, які збираються більшістю провайдерів (швидкість натискання клавіатури та миші, кут нахилу телефону, тривалість перебування у мережі тощо). Переконання, думки особи, які традиційно розглядаються частиною внутрішнього світу людини, не підлягають зовнішньому контролю в інтернеті, опиняються під суспільним наглядом, оскільки пошукові запити, «лайки» в соціальних мережах, перегляд відео, фото, інші сліди, здатні створити психологічний портер фізичної особу. Не сприяє здійсненню права на анонімність використання більшості соціальних мереж, поширення дистанційної біометричної ідентифікації, алгоритмів збору та обробки даних [776, с. 65].

Ставлення до анонімності змінилось, оскільки правовідносини у мережі «Інтернет» потребують проходження ідентифікації та автентифікації,

можливість зміни імен або використання псевдонімів, ставить все більше дискусійних правових питань, оскільки така безмежна свобода нівелює загальні засади дії цивільного права.

Як зазначає Я. Коксвік, що поряд із зручністю множинності ідентичностей у мережі «Інтернет», обов'язковою умовою участі у відносинах є використання процедури дистанційної автентифікації фізичної особи [842, с. 77] Так, у Південній Кореї обов'язковою умовою участі в онлайн-іграх є надання даних своїх національних посвідчень [609].

Ш. Теркл, будучи одним із перших фахівців, які досліджують цифрову ідентичність у контексті мультикористувацьких ігор, зазначав про її множинність та децентралізованість [838, с. 643]. Схожий підхід був висловлений і Д. Вижневським та Р. Койном у теорії масок, де ідентичність, справжнє обличчя ховається під безліччю соціальних масок, зокрема й тих, що створюються у віртуальному просторі [873, с. 191].

З технічної точки зори, анонімність у мережі завжди була відносною, водночас із початком 2000 років та настанням нового етапу розвитку інтернету, який отримав назву Web 2.0., засади анонімності та множинності ідентичності були нівельовані через просування ідей єдиної автентичної ідентичності та повної прозорості в мережі. Відтак уявлення про інтернет як простір анонімності, де особа може вільно ховатися за різними масками, а її поведінка не контролюється, втратили актуальність.

Сучасні тенденції розвитку цифрової ідентичності зводяться до презентації автентичної особи в цифровому просторі [207, с. 85]. За твердженням Х. ван Дейка, власники платформ зацікавлені у використанні автентичної цифрової ідентичності в інтернеті задля збирання та обробки якомога більшого обсягу персональних даних про користувачів, спрямування персоніфікованих новин та реклами [841, с. 199]. У 2009 році М. Цукерберг висловив зацікавленість у розвитку архітектури єдиної ідентичності та обмеження анонімності в мережі, що відображено в політиці приватності компанії [597, с. 199]. Дана позиція залишилася незмінною навіть після витоку персональних даних півтора мільярда

користувачів восени 2021 р. [888]. Корпорації спрямовують зусилля змінити цінності та звички користувачів. Просування концепція «єдиної автентичної ідентичності» або «політики реальних імен», а з тим прозорості та справжньої ідентифікації, знайшло своє відображення в технологічних рішеннях GAFAM, які спонукають користувачів використовувати реальні імена (п.1. Розділу 4 Користувацької угоди [334]). Крім того, прихильність ідеалам єдиної автентичної ідентичності та тотальної прозорості висловлюють: багаторічний редактор видання «Wired» К. Келлі[598], колишній керівник Google Е. Шмідт [559]та інші.

Сервіс блогів Twitter пред'являє вимоги дотримання умов автентичності особи лише щодо професійних облікових записів (Політика відносно професійних облікових записів [749]). Крім того, використання сервісів, які забезпечують розпізнавання обличчя та геолокацію на фотографіях Facebook та інших соціальних мережах також не сприяє анонімності (наразі обмежено використання на платформі). Тож користувачам надано можливість вимикати налаштування та забороняти компанії розпізнавання обличчя та геолокацію. На думку А. Росі, наразі фактично світові інтернет-гіганти, а не держава визначають політику розкриття користувачами своїх персональних даних[776, с. 65]. Слід зауважити, що дане висловлювання було зроблено у 2014 році, до скандалів із Cambridge Analytica та масових витоків персональних даних, які істотним чином вплинули на розробку та прийняття Регламенту ЄС 2016/679.

Так, у 2011 році письменник Салман Рушді був вимушений доводити, свою ідентичність компанії Facebook, яка поставила під сумнів, що людина, яка керує сторінкою «Салман Рушді» у Facebook є автентичним письменником. Facebook затребував у користувача профілю (який належав письменнику), підтвердити його ідентичність. Однак Рушді не зміг довести, що його ім'я – «Салман», оскільки його перше ім'я – «Ахмед», яке він подекуди використовує, а Салман – друге ім'ям. Facebook затребував перейменувати сторінку на «Ахмед Рушді». Цим випадком письменник поділився на сторінці у Twitter, на цю ситуацію звернули увагу Facebook та вирішили поступитися правилами спільноти,

задовольнили вимогу письменника, підтвердили його особистість на платформі [810].

Тож якщо на початку ери інтернету розголошувати реальне ім'я, адрес, номер телефону в інтернеті побоювалися, то зі спливом часу надання реальних, а не вигаданих даних стає запорукою довіри та засобом розбудови цифрової репутації. Адже вчинення більшості дій у мережі вимагає проведення автентифікації, ідентифікації із застосуванням номера телефону та внесенням інших персональних даних. За визначенням К.Г. Некіт, означена ситуація обумовлена поширенням принципу «послуга в обмін на персональні дані», яка використовується більшістю додатків та платформ [116, с. 57].

Наступним кроком на шляху поширення концепції єдиної автентичної ідентичності є просування технології «єдиного акаунту», який більш централізовано забезпечує компаніям можливість збирати персональні дані, поведінку особи в мережі, для чого використовується теза зручності застосування та доступу до даних. Дана технологія застосується GAFAM.

Компанії розробляють технологію «одна особа – одна ідентичність», що має забезпечити доступ до різних акаунтів на підставі підтвердження інформації з них, що дозволяє розробляти єдину децентралізовану системи автентифікації – OpenID. Використання системи дозволяє особі відвідувати різноманітні сайти та платформи, не проводячи реєстрацію на кожному [582, с. 250]. Спеціально створений Фонд OpenID проводить заходи для поширення та просування системи [723]. Можна стверджувати, що компанії намагаються запроваджувати обмеження в користувацьких угодах на вчинення анонімних дій, поряд із цим державні органи взявши на себе міжнародні зобов'язання із забезпечення прав людини намагаються забезпечити баланс між правом на приватність та забезпеченням безпеки в інтернеті

Множинність акаунтів або ідентичності тісно пов'язано з питанням анонімності. Як зазначає Я. Коксвік, користувач може не бажати асоціюватися з певною віртуальною ідентичністю у фізичному житті завдяки анонімній участі у блогах, чатах, віртуальних іграх тощо. В окремих ситуаціях збереження

анонімності є недопустимим, якщо віртуальна ідентичність завдає шкоди [842, с. 77].

З огляду на зазначене, користувачі виступають проти намагань технологічних компаній запровадити єдиний автентичний акаунт. Висувається навіть припущення, що GAFAM вимушені залишати роздільні акаунти через побоювання втратити популярність серед нових користувачів.

Ю.С. Размєтаєва звертає увагу на те, що образ, який особа транслює в мережі, впливає на здійснення її права на недоторканність приватного життя. Образ у реальному та віртуальному житті можуть не відрізнятися, також цифровий образ може принести негативні наслідки у фізичному світі [175, с. 43].

З погляду Г. Терпстра, наявність декількох облікових записів електронної пошти є лише одним із способів розділення структури життя [811, с. 15]. Більш зрілі люди схильні до фрагментації досвіду спілкування в соціальних мережах, оскільки більшість із них зізнаються про наявність двох та більше профілів[626, с. 5]. Кількість таких профілів зростає по мірі зростання кількості соціальних мереж та взаємозв’язків .

М. Кастельс [418, с. 240] та Дж. Сулер [806, с. 455] стверджують, що люди мають різні ідентичності, обумовлені ролями, які вони проявляють у суспільстві.

Множинність ідентичності в соціальних мережах дозволяє користувачам управляти профілем відповідно до вподобань віртуальної спільноти для досягнення позитивних відгуків та взаємності в інтернет-середовищі [237, с. 47].

Х. ван Дейк дослідив, як змінюється ставлення суспільства до множинності цифрових проєкції та анонімності в інтернеті. На погляд науковця, зміна архітектури соціальних мереж уособлює боротьбу платформ за набуття права контролювати ідентичність користувача. Відповідно до того, як у суспільстві люди грають різні ролі в сім’ї та на роботі, соціальні мережі покликані представляти різні проєкції: у трудових або приватних відносинах. Науковець ставить під сумнів раціональність для користувачів об’єднання на платформах єдиної автентичної цифрової ідентичності. Пряме або опосередковане примушування користувачів розкривати персональні дані є

утопічним. Розширення обсягу даних веде до збільшення персональних даних які отримують та обробляють компанії [841, с. 199].

Щодо державних систем ідентифікації Дж. Уодхам звертає увагу, що система ідентифікації заснована на принципі відповідності однієї фізичної особи – її автентичній ідентичності та автентичних персональних даних [852, с. 127].

Враховуючи викладене, на даному етапі розвитку інформаційно-комунікаційних технологій можна розрізняти цифрову ідентичність у мережі, яка повністю співпадає із фізичною особою, є автентичною, та вигаданою (фейковою), яка не дозволяє ідентифікувати користувача у відносинах із іншими в мережі. Наразі така умова залишається переважно на платформах соціальних мереж та ігор.

Визнаючи переваги множинності цифрової ідентичності та властивості репрезентації фізичної особи в мережі «Інтернет», слід зазначити, що технологія єдиної цифрової ідентичності може мати переваги у сфері спадкових відносин, дозволяючи встановлювати за життя обсяг даних, доступ до яких може бути наданий після смерті користувача. Оскільки користувачі залишають акаунти та цифрові сліди на різних платформах, про які можуть не знати спадкоємці. Технологія єдиної цифрової ідентичності має значення для сфери державних послуг та має надати право управляти своїми даними. Технологія єдиної автентичної цифрової ідентичності на платформі Блокчейн покликана забезпечити доступ до основного облікового акаунту, який відкриває доступ до інших профілів, вирішити проблему доступу до електронних грошей, криптовалюти, віртуальної власності у відеоіграх, об’єктів інтелектуальної власності, електронних документів комерційної цінності після смерті спадкодавця тощо.

Кроком на шляху формування єдиної автентичної ідентичності фізичної особи в інтернеті може стати визнання 58 державами світу електронних версій українських документів вебпорталу «Дія», що має розширити можливості використання громадянами України електронного відображення інформації, що міститься в документах, передачі електронних копій відповідних документів,

отримання публічних послуг за межами України. Для забезпечення даних нововведень передбачена передача даних демографічного реєстру та інших персональних даних громадян України до ЄС, що покликано спростити роботу державних органів, у тому числі органів, уповноважених проводити реєстрацію актів цивільного стану.

Поряд із окремими позитивними аспектами технології єдиної ідентичності, встановлення обов'язкової реєстрації та використання ПІБ відповідно до національних посвідчень у соціальних мережах та іграх, приватних платформах, є поодиноким в окремих державах, де використовується авторитарний підхід до правового регулювання відносин у мережі «Інтернет».

З урахуванням того, що на даному етапі розвитку інформаційно-комунікаційних технологій фізичні особи можуть в окремих випадках створювати фейкові акаунти, доцільно зупинитися на окремих наслідках. Сучасне програмне забезпечення характеризується потенціалом для порушення прав осіб та вчинення шахрайства із персональними даними. Компіляція фото, відео, документів за допомогою використання нейронних мереж дозволяє створювати фейки, які не відрізняються від відео із зображенням реальних фізичних осіб. Завдяки введенню в оману користувачів, вони отримали назву діпфейків [95, с. 290]. Наприклад, сучасні технології розпізнавання обличчя, мови, обробка персональних даних дозволяють створити відеопромову політичного діяча, яку він не промовляв. Технології високого рівня реалістичності значний час використовувалися у кіноіндустрії, залишалися доступними для вузького кола осіб, а створення копій застосовувалося переважно в кіноіндустрії, де використовувалося високопрофесійне обладнання. Допоки розвиток технологій не створив умови, коли додатки, які дозволяють маніпулювати із зображенням та голосом, стали доступним для широко кола осіб.

Сучасні технології генерації діпфейків забезпечують досягнення високого рівня реалістичності при створенні фальсифікованих відео на домашньому комп'ютері та смартфоні, та не потребують навичок кваліфікованих фахівців. Як

приклад можна навести програму DeepFaceLab, яка поширюється в мережі «Інтернет» безкоштовно, з детальною інструкцією для створення високореалістичних відео [15].

В основу технології створення реалістичних аудіовізуальних матеріалів діпфейк покладено різновид автоматизованої обробки ШІ та нейронних мереж. Як така, технологія компіляція зображень, відео або аудіо, є інструментом для вираження творчості, водночас може створювати умови для зловживання правом. Відео, згенеровані технологіями діпфейк, сприймаються користувачами як реальні та вводять їх в оману. Особливо відзначається поширенням використання відео, згенерованих штучним інтелектом, напередодні проведення виборів для впливу на вільне волевиявлення виборців [342]. Використання діпфейк технології поширюється в тому числі для вчинення шахрайських дій, введення в оману не лише широких верств населення, а й окремих осіб, у тому числі підміною даних для отримання доступу до системи. На тлі попереджень про використання нової технології кіберзлочинцями, за допомогою клонування голосу керівника компанії було вчинено викрадення $ 35 000 в ОАЕ [349].

З урахуванням того, що зловживання використанням технологією може нести загрозу національній безпеці, поступово приймаються нормативно-правові акти, які забороняють використання технології діпфейк у КНР та окремих штатах США [10]. У США надалі розробляються законопроєкти, направлені на притягнення до кримінальної відповідальності та накладення штрафів за використання технології діпфейків у разі створення з їх допомогою відео, фото порнографічного характеру, зображень, які сприяють поширенню насильства та відео, фото, які впливають на функціонування державних органів [54].

Слід зазначити, що неправомірне використання інформації стосовно особи, яка характеризує її фізіологічні та біологічні властивості, у разі відсутності законно наданої згоди суб’єктів даних на такий збір, обробку даних для відповідної мети, має бути визнано порушенням використання персональних даних (відповідно до ст. 5, 6, 7 Регламент ЄС 2016/679. Соціальні мережі також вживають заходи, які обмежують публікацію синтетичного контенту. Так,

TikTok у користувацькій угоді передбачає заборону розміщати маніпулятивний контент, який здатний завдати шкоди. Twitter передбачає маркування змінених новин для інформування користувачів, водночас не передбачає видалення таких публікацій. Така міра в боротьбі з маніпуляціями та фейковими новинами має підвищувати обізнаність та рівень довіри до контенту, поширюваному в мережі. Можна стверджувати, що запровадження обов'язкового маркування змінених публікацій має допомагати користувачам розпізнавати копії та підробки, сприяти зниженню дезінформації.

У боротьбу з діпфейками, які порушують права людини, може застосовуватись технологія автоматизованої обробки, яка виявляє внесення змін у фото, відео та публікації – фактчекінг (англ. fact checking – перевірка повідомлень та виявлення фейків). Технологія перевірки зміненого контенту фактчекінг є доступна на платформах, соціальних мережах та користувачам.

Також слід назвати такий спосіб обробки даних, який може порушувати права користувачів як вебскрепінг. Системи машинного навчання, в тому числі, які генерують діпфейки, використовують дані, які заходяться у відкритому доступі, звідси постає питання щодо прав на ці системи даних та законні межі вебскрепінгу. Під вебсерпінгом розуміється автоматизована обробка сторінок та систем даних у відкритому доступі, із застосуванням спеціальних ботів, не передбачає злому програмного забезпечення або атаки [781]. Так, у справі hiQ Labs Inc. v. LinkedIn Corp, яка стала ключовою в обмеженні використання, збору загальнодоступних баз даних, суд встановив межі законного вебскрепінгу та заборонив здійснювати вебскрепінг даних, розміщених у вільному доступі, зокрема на платформі LinkedIn, через те, що особа має дійсний доступ до системи, але отримує доступ до частин системи, для яких не призначена така обробка [611].

Способом припинення неправомірного використання технологій діпфейк на території України є застосування ч. 1 ст. 56 Закону України «Про авторське право і суміжні права», яка передбачає право особи звернутися до власника сайту (особи, яка володіє обліковим записом) із вимогою про видалення контенту та

припинення порушення авторського права та суміжних прав, у свою чергу відповідач зобов'язаний прийняти необхідні міри із видалення контенту протягом 48 годин із відповідним інформуванням заявника [144].

Слід зазначити, що викрадення цифрової ідентичності та її персональних даних або маніпуляції із персональними даними особи стосуються лише автентичних акаунтів (профілів) та персональних даних фізичних осіб.

Можна виокремити такі аспекти, пов'язані зі створенням діпфейків: перший аспект пов'язаний із використанням даних у машинному навчанні для введення в оману окремих осіб або суспільство, вчинення шахрайства, порушення законодавства про обробку персональних даних; другий аспект пов'язаний із тим, що в результаті використання технології, можуть створюватися похідні об'єкти інтелектуальної власності, які можуть порушувати права авторів (проблема меж порушення прав інтелектуальної власності не є предметом даного дослідження).

Ми вважаємо, що проєкти, які використовують ШІ, в тому числі генерують діпфейки, мають відповідати вимогам та стандартам аналогічно тим, які встановлюються для захисту прав споживачів по відношенню до будь-яких товарів, послуг. З огляду на те, що від прозорості функціонування залежить безпека в суспільстві, для здійснення вільного вибору, необхідно встановлення в законодавстві стандартів для функціонування систем ШІ та обов'язок їх дотримання компаніями. Системи, які генерують діпфейки або безпосередньо взаємодіють із людиною в телефонній розмові, можуть бути прикладом, коли має розкриватися інформація, що суб'єкт взаємодіє та спілкується з автоматизованою системою ШІ. Або в разі використання систем, які використовуються для аналізу емоцій та категоризації за біометричними даними, суб'єкт має бути поінформований про те, що автоматизована система ШІ збирає дані, наприклад, на прикордонних пунктах перетину. Суб'єкт має бути повідомлений про те, що взаємодіє з ШІ, інакше це є порушенням етичних норм. Наразі про обов'язок дотримуватись прозорості застосування певних систем ШІ передбачає прийнятий Акт ЄС про ШІ. Адже проблема прозорості використання

ШІ стосується: відсутності пояснення застосування алгоритмів; порушення балансу доступу до інформації; відсутність належного сповіщення про те, що особа взаємодіє із ШІ – автоматизованим нелюдським агентом; непрозорість інформації про потенційні наслідки [313].

Наступним чинником, який потребує дослідження та впливає на формування концепції цифрової ідентичності фізичної особи є репутація в мережі. З погляду А. Джонсона, цифровою репутацією можна управляти, вона є невід'ємною складовою соціальних мереж. Наразі держави, які дотримуються ліберального підходу до регулювання мережі «Інтернет», не передбачають у законодавстві суворих вимог до використання єдиної автентичної цифрової ідентичності у приватних інформаційних системах, цифрова ідентичність може як повністю співпадати з фізичною особою в мережі «Інтернет», так і не співпадати. Цифрова ідентичність у державних інформаційних системах відтворює повністю дані фізичної особи в мережі «Інтернет». А. Джонсон висуває низку досить дискусійних тез про колективний, груповий характер цифрової репутації та «цифрових ідентичностей», які належать платформам. Якщо з колективним характером цифрових ідентичностей складно погодитися, а питання прав на персональні дані наразі розробляються в науці, то постає потреба більш детального розгляду такої категорії як цифрова репутація.

Є. Кастронова в контексті багатокористувацьких ігор у мережі зазначає, що гравець, який порушує правила гри, створивши новий аватар, має створювати нову репутацію, однак нові аватари не здатні завдати шкоди. Командне або спільне виробництво, поступове просування у грі підтримує дотримання соціальних норм у ній. Різноманітні атрибути, бали заохочують гравців до розвитку та підтримання віртуальної репутації своїх аватарів. Умовою існування такої системи заохочення репутації є повільне просування та розвиток соціального капіталу в новому аватарі. Такий захід передбачений задля того, щоб користувачі не зловживали умовами та правилами спільноти [419, с.37].

М. Лемлі та Ю. Волох звертають увагу на те, що наклепи, висловлення неправдивих тверджень на вчинки аватару у віртуальному просторі можуть

завдавати шкоди репутації аватара, ускладнювати участь людини в діловому та суспільному житті з використанням аватара, та мають визнаватися порушенням прав. Науковці стверджують, що навіть якщо аватар представляє вигадану особу, використовує вигадане ім'я, це не виключає завдання йому шкоди та не позбавляє права пред'явити позов. Шкода репутації аватара, представленого під псевдонімом, може бути меншою, ніж репутації реальної людини, через незначний репутаційний капітал, ніж шкода репутації реальної особи. Однак, у різних віртуальних світах ситуація може відрізнятися, актор може бути відомий як під вигаданими іменем, так і під реальним. Науковці стверджують, що дана думка залишається не настільки очевидною, навіть для правників США [633, с. 1053].

За твердженням Т. Ділмана, категорія цифрова репутація тісно пов'язана із поняттям «цифрової довіри», яка здійснює взаємний вплив один на одного[469]. Довіра визнається вагомим чинником при виборі контрагента в мережі. Як стверджують у своїх роботах Дж. Хамарі [548], Т. Давенпорт [460, с. 2], М. Васко [855, с. 35], репутація визнається найбільш істотним показником вірогідності для вступу у відносини та співпрацю; найважливішим чинником, що мотивує до участі в онлайн-комунікації; основним елементом статусу особи в цифровій спільноті.

Згідно дослідження М. Васко та С. Фарадж, які проаналізували причини мотивації користувачів ділитися знаннями в інтернеті, таким способом вони посилюють власний репутаційний капітал та вплив у мережі [855, с. 35]. Дж. Донат підтверджує, що створення цифрової репутації мотивує користувачів для розміщення публікацій, ділитися результатами власної творчості, брати участь у спільній діяльності в мережі [486, с. 30].

Одна з ключових функцій цифрових платформ, яка дозволяє об'єднувати значну кількість користувачів, які розміщують власний контент (результати творчої діяльності), полягає у створенні та підтримці довіри між учасниками. Переважно саме платформи встановлюють правила формування репутації осіб, що взаємодіють між собою, та показники, що дозволяють її оцінити. Засоби, що

використовуються для створення та фіксації показників репутації, свідчать про її значущість у мережі.

Наприклад, підставами для блокування акаунту на Airbnb є порушення правил спільноти, надходження скарг інших користувачів, нездатність забезпечити безпеку гостей, невиконання домовленостей тощо [201]. Сервіс пошуку супутників BlaBlaCar може призупинити дію облікового запису, обмежити доступ користувача до платформи, припинити договірні відносини, якщо користувач отримав як мінімум три відгуки, середня оцінка яких становить не вище 3 бали (п.4.3.3.) [812]. Отже, в результаті спільної діяльності, споживання та користуванням мережевими засобами формування репутації, спільними стають «цифрові сліди», залишені в соціальних мережах, чатах, пошукових системах, сайтах самим користувачем, які характеризують його вподобання та звички, та в тому числі відгуки, пости, коментарі, теги інших користувачів про нього [880].

Цифрова репутація впливає на рішення, які приймаються у фізичному світі людьми або з використанням автоматизованих алгоритмів. Рішення про надання кредиту або зарахування на навчальну програму, видача стипендії можуть прийматися на основі аналізу даних у мережі. Підставою для звільнення із займаної посади працівника можуть бути світлини з вечірок у соціальних мережах. Так, американська вчителька в США втратила роботу через святкові фотографії у Facebook, на якій вона тримала келих вина та пива [476].

В умовах цифровізації роботодавці перед прийняттям на роботу звертаються до аналізу облікових записів осіб у соціальних мережах, оскільки управління та відповідальність за створення цифрового профілю лежить на користувачах. Майбутні претенденти на вакантні посади можуть проходити перевірку із залученням централізованих систем ідентифікації, аналізу різноманітних баз даних, що включають інформацію про місце проживання особи, кредитоспроможність тощо. Через те, що профіль у соціальних мережах аналізується службою підбору персоналу роботодавця та автоматизованими системами, користувачі прагнуть формувати образ, свідомо розміщати

досягнення в особистому, громадському, професійному житті, щоб це сприяло просуванню в кар'єрі. Слід визнати, що така ситуація призводить до самоцензурування користувачів, обмеження вільного вираження в мережі, особливо у випадку переслідування опозиційних висловлювань [699, с. 141].

Відтак актуалізується питання правової сутності цифрової репутації, яка формується та акумулюється специфічним чином із використанням технологічних засобів.

Відповідно до п. 26 ч. 1 ст. 1. ПК України діловою репутацією визначається сукупність документально підтвердженої інформації про особу, що дає можливість зробити висновок про відповідальність її господарської та/або професійної діяльності вимогам законодавства, а для фізичної особи – також про належний рівень професійних здібностей й управлінського досвіду, та відсутність в особи судимості за корисливі кримінальні правопорушення та злочини у сфері господарської діяльності, не знятої або не погашеної в установленому порядку [171].

У ст. 2 Закону України «Про банки та банківську діяльність» передбачено розуміння ділової репутації як – відомостей, зібраних Національним банком України про відповідність діяльності юридичної або фізичної особи, в тому числі керівників юридичної особи та власників, істотної участі в такій юридичній особі, вимогам закону, діловій практиці та професійній етиці, а також відомості про порядність, професійні та управлінські здібності фізичної особи [145].

Відповідно до ст. 94, 299 ЦК України право на недоторканність ділової репутації як особисте немайнове право належить юридичним та фізичним особам. Відповідно до п. 4 ст. 23 ЦК України в разі приниження честі та гідності фізичної особи, а також ділової репутації фізичної або юридичної особи, особа має право на відшкодування моральної шкоди. Ділова репутація є особистим немайновим благом, яке охороняється цивільним законодавством (ч.1 ст. 201 ЦК України). Приналежність ділової репутації до особистих немайнових благ гарантує неможливість її обмеження чи відібрання державою в будь-якому випадку, навіть у разі введення надзвичайного стану [56].

Відповідно до ухвали Пленуму Верховного Суду України від 27.02.2009 №1 «Про судову практику у справах про захист гідності та честі фізичної особини, а також ділової репутації фізичної та юридичної особини» під діловою репутацією фізичної особи розуміється набута суспільна оцінка її ділових та професійних якостей при виконанні нею трудових, службових, громадських чи інших обов'язків [167]. Відповідно до постанови Верховного Суду України від 18 червня 2020 р. у справі № 522/18103/14-ц гідність, честь чи ділова репутація є морально-етичними категоріями й одночасно особистими немайновими правами, яким закон надає значення самостійних об'єктів судового захисту. За визначенням суду, під гідністю слід розуміти визнання цінності кожної фізичної особи як унікальної біопсихологчіної цінності, з честю пов'язується позитивна соціальна оцінка особи в очах оточуючих, яка ґрунтується на відповідності її дій (поведінки) загальноприйнятим уявленням про добро та зло, а під діловою репутацією фізичної особи розуміється набута особою суспільна оцінка її ділових та професійних якостей при виконання нею трудових, службових, громадських чи інших обов'язків [158].

Відтак ділова репутація розглядається переважно як об'єкт охоронних правовідносин у випадку поширення відомостей, які можуть бути ганебними, не відповідають дійсності. Водночас через специфіку мережі «Інтернет», треті особи шляхом вчинення шахрайських дій, зламу та отримання доступу до акаунту, сторінок, електронної пошти можуть спаплюжити репутацію її власника, розсилаючи листи або вчиняючи інші дії з метою безпосередньої компрометації особи в мережі. Заволодівши чужим акаунтом у соціальних мережах, форумах, блогах, онлайн-платформах зловмисники можуть залишати негативні відгуки, які дискредитують особу в очах підписників та інших користувачів.

Слід зазначити, що з урахуванням розвитку соціальних мереж та шерингових платформ, розуміння репутації в інтернеті виходить за межі лише суспільної оцінки ділових, професійних якостей та здібностей фізичної особи, яке охоплюється категорією «ділова репутація», також репутація, яка

формується в мережі, обумовлюється оцінкою якостей особи, які персоніфікують її не лише поміж фахівців галузі, а й решти користувачів на платформі. Тож можна стверджувати, що цифрова репутація виходить за межі характеристики та оцінки лише ділових та професійних якостей, а впливає на можливість участі в комунікації та договірних відносин як у мережі, так і у фізичному світі, виходячи за межі охоронних правовідносин. Слід звернути увагу, що оцінка якостей та здібностей особи в цифровому середовищі може впливати на можливість участі в договірних відносинах у фізичному світі. Так, велика кількість підписників у фотографа, відеорежисера, художника, спікера, який веде популярну сторінку в соціальній мережі, привертає рекламодавців, організаторів заходів, клієнтів тощо для укладення договорів у фізичному світі.

Фахівці в галузі управління цифровою репутацією називають такі ризики, які можуть заплямувати репутацію в інтернеті: 1) негативні відгуки незадоволених клієнтів; 2) неправдива інформація, яка швидко поширюється в інтернеті; 3) кіберзалякування, коли зловмисники цілеспрямовано переслідують особу, завдаючи шкоди не лише репутації, а й емоційному стану; 4) витік персональних даних, який може призвести до крадіжки даних і зашкодити репутації [865].

Розглядаючи механізми, які існують для видалення або виправлення інформації в інтернеті, постає питання у виборі засобів захисту та застосування відповідальності за завдання збитків репутації в інтернеті, яке перетинається із такими цінностями як свобода вираження поглядів, публічними інтересами та історичною цілісністю.

Безумовно для захисту від злочинних наклепів можливим є використання дифамаційного позову та публічне спростування висловленої інформації [786]. В.М. Шкабаро, Т.А. Тодорашко, А.В. Біла називають такі спеціальні способи захисту ділової репутації в мережі «Інтернет» як: спростування достовірної інформації або право на відповідь; заборона поширення інформації, якою порушуються особисті немайнові права [282, с. 78]. До вимог відносно спростування та заборони поширення недостовірної інформації в мережі

«Інтернет», розміщеної в засобах масової інформації, встановлюється спеціальна позовна давність, яка складає один рік (п. 2 ч. 2 ст. 258 ЦК України). У такому випадку позовна давність обчислюється від дня розміщення цих відомостей у засобах масової інформації або від дня, коли особа довідалася чи могла довідатися про ці відомості. Сплив позовної давності без поважних причин, про застосування якої заявлено стороною у спорі, до винесення судом рішення, є підставою для відмови в позові.

У випадку відсутності інформації про особу порушника, який поширив недостовірну інформацію, місце проживання (місцезнаходження) неможливо встановити, оскільки залишення публікації на сайті є вільним та анонімним, відповідність покладається на власника сайту, де розміщенні публікації, який визнається належним відповідачем, завдяки створеним технічним можливостям та умовам поширення недостовірної інформації. Дані, кому належить сайт, можуть бути витребувані згідно з положенням ЦПК України в адміністратора системи реєстрації та обліку доменних імен та адреси українського сегмента мережі «Інтернет» [62]. У випадку, якщо недостовірні дані, які порочать гідність, честь чи ділову репутацію, розміщені в мережі «Інтернет» на сайті, зареєстрованому як засіб масової інформації, то до таких порушників застосовуються норми законодавства, які регулюють діяльність засобів масової інформації.

Через специфіку відносин у мережі, ступінь шкоди, що може бути завдана репутації в інтернеті, може бути настільки істотною, що особа ризикує втратити роботу, бути виключеною друзями, стати ізгоєм, коли: застарілі факти персональної біографії поширюються в мережі; відео стають вірусними; у пошукових результатах з'являються неактуальні, застрілі новини про притягання особи до відповідальності тощо. Подібне поширення фактів ладне істотними чином зіпсувати життя особи у фізичному світі, та навіть довести до самогубства. Так, італійка не витримала жартів та образ, вчинила самогубство через рік після того, як відео приватного характеру з її участю було поширено в мережі та стало вірусним[69]. У 2013 році громадянин США, придбавши гамбургер та будучи

невдоволеним якістю проданого товару, кинув його у вагітного продавця, відвідувачі закладу опублікували записане відео, яке стало вірусним у мережі. Не витримавши психологічного тиску на роботі, фінансово виснажений чисельними судами щодо видалення контенту, навіть отримавши рішення на його користь, він вчинив самогубство на Мангеттені через неможливість позбутися тіні кинутої на його репутацію.

Можна стверджувати, що людина у фізичному світі стає певною мірою залежною від відгуків третіх осіб, фото та відео з нею можуть потрапити в мережу та вплинути на цифрову репутацію. Майже миттєве поширення відео в мережі або його віральність свідчить про одночасне споживання користувачами контенту в мережі. Крім того, вищезазначені приклади є підтвердженням мережевої структури відносин та наростаючої взаємозалежності між фізичними, юридичними особами та інформаційними технологіями.

Поряд із судовим порядком захисту репутації в мережі, шляхом подання позову про захист честі, гідності та ділової репутації, спростування недостовірної інформації та відшкодування моральної шкоди наразі отримує поширення застосування позасудового порядку, шляхом направлення листа до відповідного сервісу, який поширює контент із порушенням (розміщує недостовірну інформацію, порушує авторські права) з вимогою про видалення відповідної інформації [57].

Поряд із правом на видалення, через зростаючу проблему зловживання правом в інтернеті, сервіси передбачають у користувацьких угодах право суб'єктів вимагати видалення, навіть ширшого переліку публікацій, ніж це передбачає право на видалення. Така можливість є досить зручною в державах, які безпосередньо передбачають у законодавстві право на видалення, наприклад, у Канаді, де так звані сайти помсти та ганьби повторно публікують рішення судів із зазначенням ПІБ порушників та посиланням на їх акаунти [190].

Відповідно до умов користувацької угоди Twitter забороняється публікація приватної або конфіденційної інформації іншої особи, включаючи інтимні фото або відео, які були зроблені або поширені без її згоди [747]. Reddit забороняє

розміщення відвертих фото та відео, зображення оголеного тіла, поведінки приватного характеру та розміщення персоналізованих зображень насильницького характеру, які підлягають видаленню[748]. Відповідно користувацької угоди TikTok, забороняється розміщення зображень приватного характеру без згоди особи та застережується, що розміщення публікацій відвертого характеру може стати підставою для притягнення до відповідальності в багатьох державах[253]. Facebook передбачає у користувацькій угоді заборонені різновиди контенту, серед яких як зображення сцен насильства, мови ворожнечі, сексуальних домагань та зображення оголеного тіла[85]. Сервіс передбачає порядок видалення контенту, який містить зображення приватного характеру, зображення насильницьких дій, поширені без згоди користувача. Youtube передбачає заходи блокування контенту, обмеження доступу до певних функцій, обмеження можливості монетизації та отримання доходу від каналу у випадку порушення правил спільноти або порушення авторських прав, що безпосередньо впливає на цифрову репутацію облікового запису [66]. Відтак у разі порушення правил цифрової спільноти, користувач, який прагне помститися, опублікувавши відео, фото образливого контенту, ладен зіпсувати репутацію не лише іншій особі, а й заплямити свою репутацію, втративши можливість використання та монетизації власного каналу. Історія минулих дій або транзакцій, бувши частиною профілю фізичної особи, може бути використана для комерційних або правоохоронних цілей, та впливати на здатність особи вчиняти дії в межах інформаційної системи.

Отже, в умовах цифровізації дані про особу, її життя та вподобання змінюють значення. З огляду на норми Регламенту ЄС 2016/679 дані, будучи переданими та зафіксованими в інформаційних системах можуть передаватися з однієї платформи до іншої, набуваючи самостійної економічної цінності, навіть набуваючи ознак товару (для цілей таргетованої реклами тощо), що ставить питання визнання їх як немайнового об’єкта цивільних відносин. Слід зазначити, що збір та обробка персональних даних користувачів відбувається незалежно від того, чи є акаунт відкритим або закритим. Тому постає питання визначення місця

цифрової репутації в системі об'єктів цивільних прав. Слід зазначити, що сукупність даних про людину, розміщених і поширених у мережі «Інтернет», не лише характеризують її, а й формують репутацію, дозволяють провести її ідентифікацію, зокрема як потенційного учасника відносин платформ спільного споживання.

Поряд із формуванням репутаційного рейтингу, який формується на базі приватних платформ та соціальних мереж, слід відзначити підхід до формування репутаційного капіталу та створення системи соціального кредиту державними органами та соціальними мережами, як рейтингова система КНР. Ідеологом розробки системи соціального кредиту в КНР вважається Чж. Юнкан, міністр державної безпеки КНР початку нульових, заарештований у подальшому за звинуваченням у корупції та довічно ув'язнений. Саме його ідеї створення системи суспільного управління, заснованої на оцінці правомірності поведінки громадян були покладені урядом КНР для посилення державної безпеки та забезпечення стабільності за допомогою застосування інформаційно-комунікаційних технологій нагляду для розробки системи соціального кредиту та створення проєкту «Великий китайський фаервол» або «Золотий щит»[657, с. 5]. Система соціального кредиту КНР відрізняється від аналогічних систем решти держав тим, що збирає як дані про особу з державних офіційних реєстрів – це освіта, соціальне страхування, фінансовий стан, кредитні зобов'язання, об'єкти власності, так і дані соціальної комунікації: соціальний статус та особисте життя. Ця система дозволяє будувати, «заробляти» власною позитивною поведінкою кожному громадянину КНР певний рейтинг, доступ до соціальних благ, послуг, що надаються через дозвільні та заохочувальні механізми держави. Система аналізує великі дані з усіх доступних джерел. Сутність соціального кредитування в КНР полягає в тому, що виступає інструментом оцінювання. У КНР використання системи соціального кредиту є відкритим та прозорим для фізичних осіб, є частиною державної політики, інструментом публічного управління, покарання та заохочення. Соціальне кредитування в КНР використовує системи обробки великих даних. Досвід КНР

свідчить, що законодавство може формувати соціальний рейтинг на підставі збору, обробки даних, профілювання фізичних осіб та градації в залежності від оцінки вчинків особи. Можна припустити, що характерною властивістю рейтингової системи КНР, у порівнянні з аналогічними у світі, є її виховний характер.

Щодо ЄС, то з прийняттям Акту ЄС про ШІ, використання систем соціального рейтингу, оцінки та прогнозування соціальної поведінки фізичних осіб віднесено до діяльності із високими ступенем ризику та повністю заборонено (відповідно до ст. 113 Акту ЄС про ШІ) [313].

У США діє платформа Data Services Hub, відповідно до Закону про доступне медичне обслуговування, яка збирає дані про фінансовий стан, кредитну історія, трудову діяльність, стан здоров'я та дані про соціальне забезпечення, місце проживання та громадянство, притягнення до відповідальності та судимості осіб, які мешкають на території США [441]. Дані акумулюються від Служби внутрішніх доходів, Служби охорони здоров'я та соціальних служб, Міністерства внутрішньої безпеки, Департаменту юстиції та інших органів штаті. Планується передання даних від Міністерства оборони, Міністерства у справах ветеранів, Офісу управління персоналом, Корпусу миру та даних Федеральної програми США, яка забезпечує оплату медичних витрат соціально незахищеним верствам населення. Такі дані про фізичних осіб є досить цінними для компаній. Доступ до даних Data Services Hub має надаватися урядовим організаціям, суб'єктам підприємницької діяльності, які отримали ліцензії на доступ, пов'язаний з конкретним видом їх діяльності.

Відтак цифрова система рейтингу пов'язана з тим, що беруться до уваги вчинки та правочини, вчинені не лише на цифрових платформах, а й належне виконання договірних домовленостей із фінансовими установами, що обліковують надійність позичальників.

Від початку тризначний рейтинг кредитоспроможності було розроблено у 1956 році компанією Fair, Isaac & Co. (наразі FICO), який по суті був прогнозуванням вірогідності невиконання позичальником своїх зобов'язань із

повернення кредиту [658]. М. Фуркад та К. Хілі зазначають, що система кредитного рейтингу призвела до революційних зрушень у підприємницькій діяльності, оскільки з другої половини XX століття банки США стали передавати оцінку платоспроможності майбутніх контрагентів спеціалізованим фінансовим компаніям та фахівцям. Зміна вимог вплинула на споживачів, які стали вимушеними підлаштовувати власні біографічні дані та показники, щоб створювати сприятливе враження про себе для фінансових установ [523, с. 23]. Особливістю вищезазначених систем у США є спрямованість на формування довіри у сфері фінансових послуг.

Відносно України, наразі законодавство не містить визначення соціального кредиту, а поняття кредитної історії передбачено ст. 3 Закону України «Про організацію формування та обігу кредитних історій». Згідно з даною статтею, кредитна історія – це сукупність інформації про юридичну або фізичну особу, що її ідентифікує, відомостей про виконання нею зобов'язань за кредитними правочинами, іншої відкритої інформації відповідно до Закону[162]. Джерелами формування кредитних історій є: відомості, що надаються Користувачем до Бюро за письмовою згодою суб'єкта кредитної історії відповідно до даного Закону; відомості державних реєстрів, інформація з інших баз даних публічного користування, відкритих для загального користування джерел за винятком відомостей (інформації), що становлять державну таємницю (ст. 5 Закону).

Ми вважаємо, що системи (рейтингу) довіри або обліку репутації та система соціального (кредиту) можуть розглядатися як різні підходи до формування цифрової репутації. Перший підхід застосовується у США та ЄС, передбачає створення рейтингу довіри та системи обліку репутації, яка обліковується цифровими сервісами та шерінговими платформами як Facebook, Airbnb тощо. Цифрова репутація є, певною мірою, фрагментарною, оскільки її показники розміщуються на різних платформах. Поряд із цим, платформи надають сервіси для підрахунку відвідуваності сторінок користувачів, що створює умови для прозорості цифрової репутації в мережі У. свою чергу

рейтингові системи довіри, які формуються органами державної влади та фінансовими установами, передбачають певну централізацію. Дані системи не є системами соціального рейтингу (кредиту), а спрямовані на формування прозорості та довіри в цивільних відносинах. Відповідно другий підхід, який набув реалізації у КНР, передбачає відносно централізований державний контроль у проведенні оцінювання вчинків та формування соціального рейтингу за допомогою оцінки великих даних. Особливістю китайської системи є те, що поряд із реалізацією державної політики та владних повноважень органами влади, провадиться ретельне регулювання мережі та комунікації між суб'єктами та технічними засобами. Система соціального рейтингу об'єднує системи довіри фінансових установ, державних органів, вчинків у соціальних мережах та фізичному світі тощо. За результатами соціального рейтингу можуть наставати юридично значущі наслідки.

Можна підсумувати, що профілювання, яке застосовується в соціальному кредитуванні, містить особисті дані, здатні розкрити вразливі вади фізичної особи, стати інструментом маніпулювання. Крім того, система соціального кредитування передбачає застосування оцінки за дії та бездіяльності фізичної особи, що може нести юридично значущі наслідки (покарання або заохочення), що неминуче веде до пристосування суб'єкта до заданих вимог. Проблемою застосування соціального кредитування, обробки та аналізу вчинків із застосуванням автоматизованих систем є дискримінація, яка може в результаті здійснення нею прав та обов'язків виникати та впливати на фізичну особу.

Можна припустити, що цифрова репутація могла б стати основою для створення персонального бренду фізичної особи, під яким мав би розумітися образ, обіцянки та очікування, які виникають у свідомості інших людей. Аналогічно персональному бренду, який створює асоціацію з певним товаром, продуктом або виробником у споживача, який мав би включити поряд із репутацією, поведінку, навички, імідж, які свідчать про неповторність та унікальність[529, с. 99]. У разі дотримання такої позиції, що кожен персональний бренд відрізнятися від інших та сприймається як новий, оригінальний[884, с.

1352], то можна припустити, що платформи в мережі дозволяють створювати неповторний засіб індивідуалізації суб'єкта, на який може бути поширений режим інтелектуальної власності. У разі дотримання такої позиції щодо визнання за цифровою репутацією виключного (немайнового) права, постає питання визначення її правовласника, забезпечення застосування способів захисту у випадку правопорушення, забезпечення належної охорони бренду як складного об'єкта та її складових елементів, цифрової репутації. Водночас у цьому разі потрібна розробка та законодавче закріплення ознак і умов, що дають підставу для визнання певної сукупності даних про людину та інших даних, що характеризують її, особистим брендом та умов, коли ці самі дані можуть зберігати значення самостійних об'єктів цивільних прав поза особистим брендом. На наш погляд, на даному етапі розвитку мережі цифрової репутацією елемент бренду фізичної особи, який їй належить як виключне (немайнове) право, не представляється можливим.

Цікаве твердження висловив у 2005 році С. Кроуфорд, що цифрова репутація набуває ознак результату колективної діяльності. В умовах шерингової економіки цифрова репутація стає груповим проєктом, а права власності на таке колективно створене нематеріальне благо ідентичності належить (за замовчуванням) онлайн-посередникам. Науковець навіть стверджує, що не лише цифрова репутація, а й цифрові ідентичності є груповими проєктами, що належать (за замовчуванням) онлайн-посередникам. Що актуалізує питання контролю та управління за онлайн-ресурсами та покладення правоволодіння за спільним онлайн-простором ідентичностей в умовах спільного створення ресурсів в інтернеті, правил щодо ідентичності у віртуальних світах [445, с. 2].

На наш погляд, при визначенні цифрової репутації необхідно брати до уваги, що більшість цифрових платформ із відгуками та рейтингами, коментарями надають право видаляти відгуки та інший контент особі, яка їх завантажила (Facebook, Google, Booking, Tripadvisor, Youtube). Саме така умова платформ та сайтів із відгуками створила умови для розвитку послуг з управляння репутацією в мережі [542]. Приклади КНР свідчать, що система

рейтингу поширюється на всі сфери життя та дає можливість впливати на рейтинг шляхом вчинення позитивних вчинків (допомога особам похилого віку, здача крові, благодійна діяльність тощо), які дозволяють підняти рейтинг та отримати доступ до матеріальних благ [600].

При визначенні правової кваліфікації відгуків, коментарів про якість послуг, товарів та робіт фізичних та юридичних осіб, які залишаються на цифрових сервісах, які можуть у поєднанні з іншими ідентифікаторами (посиланням на акаунт, ім'я, фото) ставати персональними даними та виступати складовою цифрової ідентичності, слід виходити з того, що суб'єкту належить право управління цифровою репутацією, право захисту від неправдивих висловлювань та право на їх спростування, право на забуття (видалення).

Підсумовуючи викладене, можна зазначити, що застосування систем соціального кредитування може охопити досить широкі сфери суспільних відносин. Впровадження соціального кредитування пов'язано з побоюванням створення цифрової диктатури, контролю за доступом до благ та ресурсів. Державні органи, можуть обґрунтовувати застосування соціального кредитування тезами про необхідність забезпечення безпеки в суспільстві. У разі загального запровадження соціального кредитування по відношенню до фізичних осіб, буде лише свідченням істотних зрушень та трансформацій цінностей у суспільстві в бік авторитаризму.

Застосування алгоритмів обробки та аналізу даних автоматизованими системами залишаються непрозорими для фізичних осіб. Розглядаючи етично-правові аспекти застування профілювання, з тим і соціального оцінювання, залишається питання, наскільки об'єктивним може бути оцінювання вчинків фізичної особи із застосуванням автоматизованих систем, недопустимість закріплення негативної оцінки фізичної особи пожиттєво. З метою забезпечення прав людини в умовах посилення процесів автоматизації, з урахуванням заборони використання систем соціального рейтингу та оцінки соціальної поведінки фізичних осіб в ЄС, така норма має бути закріплена у законодавстві України.

2.3. Ідентифікація фізичної особи у відносинах у мережі «Інтернет»

Індивідуалізація та належна ідентифікація особи дозволяє ефективно здійснювати права та обов'язки, реалізовувати право власності, застосовувати правові механізми захисту прав на випадок порушення. Належна ідентифікація особи, підтверджена посвідченням встановленого законодавством зразка, є умовою легального існування, адже відсутність документів, що посвідчують особу, часто пов'язана зі злочинною можливістю для особи стати жертвою работоргівлі, крадіжки персональних даних. Належна індивідуалізація фізичної особи є запорукою легітимної участі в цивільних відносинах, здійснення майнових та особистих немайнових прав та обов'язків.

Зважаючи на це, відповідно до Цілі 16.9 ООН у сфері сталого розвитку передбачено, що до 2030 року всі особи мають отримати правову ідентичність. Метою документа є не лише підвищення обізнаності про роль, яку відіграє ідентичність людей у здійсненні прав та обов'язків, а й сприяння належної реєстрації та отримання цифрових посвідчень [358].

Індивідуалізація особи є необхідною умовою її повноцінної участі у правовідносинах. З погляду В.Н. Мортези, розв'язання правових питань, пов'язаних із віртуальною ідентичністю в мережі «Інтернет» має вирішити низка заходів. По-перше, оскільки в реальному світі кожна особа при народженні має бути зареєстрована в уповноважених органах, умовою визнання особисті або цифрової ідентичності, отримання цифрового громадянства має стати формальне та юридичне обов'язкове цифрове свідоцтво про народження в цифровому просторі для всіх. По-друге, для юридичного визнання цифрової ідентичності в мережі доцільно запровадження електронної або віртуальної системи юридичної реєстрації, яка аналогічно функціонує у фізичному світі. Подібно тому як уповноважені органи (в Україні РАЦС) у фізичному світі мають проводити державну реєстрацію актів цивільного стану, відповідна система реєстрації має бути запроваджена в мережі «Інтернет». Неминучим стає для майбутнього

правового віртуального світу розробка системи реєстрації, яка аналогічна традиційній системі реєстрації, де кожному користувачу інтернету надається унікальне віртуальне посвідчення особи або віртуальне свідоцтво про народження особи в інтернеті, а також надається можливість контролювати та переглядати віртуальні посвідчення. По-третє, для підтвердження особи та автентифікації особи в кіберпросторі, впроваджується електронний підпис або кваліфікований електронний підпис. Перелічені науковцем заходи є низкою ідентифікаторів, які дозволяють провести ідентифікацію особи в мережі.

Слід зазначити, що законодавець в Україні не використовує термін «індивідуалізація» по відношенню як до фізичних, так і до юридичних осіб. Проте, підручники та навчальні посібники з цивільного права містять окремі параграфи або розділи з відповідною назвою. Так, у науковій літературі категорія «індивідуалізація» застосовується по відношенню до фізичних осіб. Фізична особа як учасник цивільних правовідносин має низку суспільних та природних ознак і властивостей, які певним чином індивідуалізують його та впливають на його правове становище.

М.О. Стефанчук у межах дослідження розглядає індивідуалізацію як процес наділення фізичної особи сукупністю певних ознак, що ідентифікують її з-поміж інших фізичних осіб і визначають її унікальність та неповторність як суб'єкта цивільних правовідносин [202, с. 116].

Н.В. Волкова наголошує, що індивідуалізація фізичної особи може здійснюватися для реалізації різних завдань: формальне виокремлення та відособлення особи; соціальна індивідуалізація особи як учасниці міжособового спілкування без вступу у правовідносини; індивідуалізація фізичної особи для встановлення можливості бути учасником правовідносин [26, с. 238; 27, с. 8].

За визначенням Р.Б. Шишки, індивідуалізація фізичної особи включає унікальні особисті ідентифікаційні ознаки, притаманні лише для неї та відрізняють її від інших. Засоби індивідуалізації можуть бути необхідними і факультативними. Необхідними є ті, що вимагаються чинним законодавством для даного виду правовідносин. Наприклад, при подані позову або подачі заяви

до органів державної влади має бути вказаний заявник, водночас автор літературного твору може оприлюднити твір анонімно або під псевдонімом [279, с. 49].

Як було з'ясовано в попередньому підрозділі, участь у правовідносинах в мережі «Інтернет» вимагає обов'язкової ідентифікації суб'єкта. А для деяких суб'єктів даних, а саме публічних осіб (акторів, співаків, державних діячів тощо), платформа може вимагати підтвердження особи, як наприклад, у соціальних мережах, у випадку створення офіційного профілю. У мережі «Інтернет» ідентифікаційними ознаками особи виступають ідентифікатори або персональні дані, які дозволяють ідентифікувати фізичну особу у віртуальному середовищі, та з огляду на їх особливий статус підлягають правовому захисту.

Значення ідентифікації в умовах розвитку інформаційно- комунікаційних технологій очевидна з огляду на те, що традиційні методи ідентифікації, коли суб'єкти знаходяться на відстані один від одного, не відповідають потребам інформаційного суспільства, до того ж відсутня загальна ієрархічна термінологія та єдині вимоги до суб'єктів правовідносин.

Необхідність розробки системи цифрової ідентифікації для зменшення витрат на укладення правочинів вказується у доповіді «A Blueprint for Digital Identity» 2016 року [292].

Поширення електронних розрахунків обумовлює розвиток законодавства про платіжні системи та застосування заходів із протидії легалізації (відмиванню) доходів, отриманих злочинним шляхом, та фінансуванню тероризму. Набуває значення електронна ідентифікація особи при наданні державних та банківських послуг в електронному вигляді, внаслідок якої проявляється потреба у надані особою та органами держави інструменту для безпечної ідентифікації особи за допомогою мережі «Інтернет».

Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» передбачає спрощену ідентифікацію в галузі фінансових послуг, а саме з 28 квітня 2020 року

верифікація банками не вимагає особистої присутності клієнта та допускає застосування способів віддаленої ідентифікації [156].

Про необхідність розвитку зручної, безпечної та доступної електронної ідентифікації як передумови запровадження електронних послуг, електронної комерції та електронної взаємодії учасників економічних взаємовідносин наголошується у Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки, схваленої Розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р [81].

Категорії «індивідуалізація» та «ідентифікація» є тісно пов'язаними. Основною метою цивільно-правової індивідуалізації М.К. Галянтич, О.О. Гармаш [32, с. 37], О.О. Кулініч [92, с. 159] називають виокремлення особи поміж інших суб'єктів цивільних відносин. В.Н. Мортеза розуміє під ідентифікацією – сукупність характеристик, поведінкових, соціальних та особистих властивостей особи, що служить її ідентифікації та відмежовуванню поміж інших осіб. Ідентичність подібна свідоцтву про народження особи, яке дозволяє її ідентифікувати поміж інших осіб [675, с. 4]. Є.О. Мічурін не проводить відмежування між категоріями «індивідуалізація» та «ідентифікація» 107, с. 91].

Доцільно розглянути, що розуміється під ідентифікацією в доктрині і законодавстві, цілей її застосування, які засоби використовуються для її здійснення та її значення в умовах розвитку штучного інтелекту, віддаленої біометричної ідентифікації, біотехнологій, інтернету речей, індустріального інтернету та інших технологій.

Попри те, що законодавство не містить визначення індивідуалізації, міститься визначення процедури «ідентифікації особи» та «електронної ідентифікації». Розвиток банківських послуг, медицини, адміністративних послуг в електронній формі, цифрової торгівлі, транскордонних взаємин із представниками бізнесу в рамках єдиного правового цифрового простору та прийняття Регламенту ЄС № 910/2014 Європейського Парламенту та Ради від 23.07.2014 Про електронну ідентифікацію та довірчі послуги для електронних

транзакцій у межах внутрішнього ринку [151], стимулювали до прийняття Закону України «Про електронну ідентифікацію та електронні довірчі послуги» [152]. Відповідно пп. 9, 20, 21 ч. 1 ст. 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» процедурою ідентифікації особи визнається використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи. Електронна ідентифікація Законом визначається як процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи. Під ідентифікаційними даними особи розуміється унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи. Аналогічне визначення електронної ідентифікації міститься в п. 14.1.56-1 ст. 14 ПК України [171] та Концепції розвитку системи електронних послуг в Україні, схваленої розпорядженням Кабінету Міністрів України від 16.11.2016 р. № 918-р [80].

К. Саліван звертає увагу на відмежовування ідентифікації та цифрової ідентичності, під якою розуміє цифровий профайл або обліковій запис (акаунт). Ідентифікація будучу однією з дій, процесу започаткування ідентичності, де першою – є ідентифікація та автентифікація особи в момент реєстрації, а друга – верифікація для встановлення автентичності особи. Інформація, зібрана під час реєстрації, використовується для автентифікації особи, встановлення її тотожності із даними. Науковець стверджує, що ідентичність перевіряється шляхом перевірки системою інформації, яка пред’являється в момент вчинення правочину із даними, що містяться в реєстрі. У момент вчинення правочину, проведення транзакції, посвідчення, яке пред’являє особа, являє собою токен, тобто символ або свідоцтво, яке служить доказом автентичності особи в цій системі [803, с. 25].

Можна назвати декілька способів ідентифікації, які передбачають різні способи організації доступу до інтернету. Найпростіший передбачає

використання реєстраційних форм, (введення даних у вільні необхідні поля, підтвердження обрання та відправка на сервер) згідно з доведеними до відома користувачами, умовами використання інтернет-ресурсу розглядається як підтвердження достовірності введених даних. Особа може ввести й недостовірні дані, якщо сервіс та законодавство не вимагає надання посвідчення особи державного зразка. Наступним способом є ідентифікація, яка забезпечує дієві гарантії можливості ідентифікації користувача з необхідністю підтвердження акаунта шляхом введення коду з повідомлення на мобільний телефон або двофакторна автентифікація. Тож можна говорити, що ідентифікація осіб в інтернеті може носити імперативний та факультативний характер.

Ідентифікація в інтернеті характеризується очевидними відмінностями від ідентифікації у фізичному житті через присутність спеціальних суб'єктів – інформаційних провайдерів (посередників), які володіють технологічною інфраструктурою, зберігають та обробляють дані відносно фізичних осіб та їх поведінки. Доступ провайдерів до даних суб'єктів створює умови «відносної ідентифікації», пов'язаної з питанням визначення відповідальності інформаційних провайдерів (посередників) та питанням, за яких умов вони мають право розкривати дані про власних клієнтів та користувачів. Розкриття інформаційним провайдерам даних про власних користувачів призводить до абсолютної ідентифікації, коли суб'єкт стає ідентифікований не лише для ідентифікуючої особи, але й для інших суб'єктів.

Вагомий вплив на формування практики в даній сфері справило рішення ЄКПЛ Delfi AS v. Estonia. ЄКПЛ відзначив важливість онлайн-анонімності для вільного вираження ідей та поглядів та особливість інтернету як безпрецедентного засобу поширення інформації, та дав характеристику ступеням анонімності в мережі «Інтернет». Суб'єкт може залишатися анонімним для широкого загалу, але при цьому ідентифікуватися постачальником послуг за допомогою облікового запису, реєстрації або контактних даних, які можуть не перевірятися або підлягати перевірці шляхом повного обмеження верифікації (шляхом активації облікового запису за допомогою адреси електронної пошти

або облікового запису соціальної мережі), так і повної автентифікації, використанням національних електронних посвідчень або за допомогою онлайн-банкінгу. Поряд з цим постачальник послуг може допускати повну анонімність суб'єктів, коли користувач не зобов'язаний ідентифікувати себе загалом та його поведінка може відстежуватися певною мірою через дані, які зберігаються провайдером доступу до інтернету. Означені персональні дані можуть бути розкриті за умови належного припису уповноважених правоохоронних органів або суду, а право на анонімність у цьому випадку може бути обмежено, коли потребує виявлення та переслідування винних осіб [380].

У справі Delfi AS v. Estonia, суд відхилив посилання заявника на ст. 10 («Свобода вираження переконань») ЄКПЛ. Дане рішення ЄСПЛ було піддано критиці міжнародними правозахисними організаціями, які припустили, що подібні прецеденти можуть привести до прийняття в ЄС законів, які будуть зобов'язувати користувачів реєструватися в інтернеті під реальними іменами [301].

Наразі GAFAM просуває тенденцію до реєстрації саме за реальними, а не вигаданими іменами користувачів. Вживаються заходи, спрямовані на прозорість діяльності в мережі, які трансформують уявлення про межі анонімності та приватності. Крім того, в межах заходів боротьби з поширенням Covid-19, оператори зв'язку зобов'язалися передавати Європейській Комісії дані про геолокацію з мобільних пристроїв своїх абонентів у березні 2020 року. З цього приводу Європейський комісар із захисту персональних даних висловив занепокоєння щодо передачі телекомунікаційними компаніями даних про геолокацію користувачів та недопущення, щоб така передача даних стала регулярною практикою [212, с. 605].

Відтак мережі «Інтернет» властива відносна анонімність для широкого загалу користувачів, обумовлена властивостями інформаційних систем, доступом постачальників телекомунікаційних послуг до персональних даних користувачів, які можуть бути передані уповноваженим органам для подальшої ідентифікації осіб у разі вчинення правопорушення [212, с. 607].

На сьогодні більшість правил користування сервісами та норми законодавства ЄС та США не передбачають вимоги повної ідентифікації особи в мережі «Інтернет», доки ця особа не вступить у правовідносини, не вчинить юридично значущі дії та не укладе правочин. Водночас кожного разу відвідуючи сторінку, натискаючи «Прийняти» у віконці «Управління згодою на зберігання кукі», користувач погоджується на використання кукі-файлів та проведення відносної ідентифікації. На сучасному етапі розвитку інтернету, платформи використовують файли кукі для збору аналітики про користувачів. Більшість таких файлів збирає, обробляє та зберігає цінні фрагменти даних, таких як клієнтський ідентифікатор відвідування сайту з браузера, за яким особа ідентифікується кожного разу, відвідуючи сторінку [287]. Отож, у звітах Google Analytics користувачі співвідносяться не з конкретним суб'єктом даних, а з конкретним клієнтським ідентифікатором. Такий захід обумовлений забезпеченням недоторканності приватного життя та складовою концепції приватності за замовчуванням.

Поряд із категорією «ідентифікація», Концепція розвитку системи електронних послуг в Україні схвалена розпорядженням Кабінету Міністрів України від 16 листопада 2016 р. № 918-р містить визначення автентифікації як електронного процесу, який дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної, телекомунікаційної, інформаційно-телекомунікаційної системи, а також походження та цілісність електронних даних [80].

Проводячи різницю у процедурах ідентифікації та автентифікації, під ідентифікацією розуміється процедура, за результатами вчинення якої для суб'єкта ідентифікації виявляється його ідентифікатор, який однозначно визначає суб'єкта в інформаційній системі, у свою чергу, під час процедури автентифікації здійснюється перевірка автентичності користувача шляхом порівняння введеного ним пароля з паролем, збереженим у інформаційній системі, що дає змогу отримати авторизований доступ до інформації та системи. З точки зору безпеки акаунта, автентифікація є найістотнішою процедурою.

Авторизація являє собою надання визначеній особі або колу осіб права на виконання визначених дій. Автентифікація без попередньо проведеної ідентифікації не має сенсу, поки система не переконається у автентичності особи яка підлягає перевірці. Процедура ідентифікації без автентифікації також не має сенсу, оскільки для того, щоб увійти в систему, особі недостатньо ввести логін, який може бути відомий третім особам, а необхідно ввести пароль. У свою чергу, авторизація без ідентифікації та автентифікації цілком вірогідна, так як передбачає надання доступу, наприклад, публікацію документів в Google Docs для широкого кола осіб. За таких умов особа володілець файлу побачить позначку про те, що файл читає невідома особа, водночас авторизована, адже їй надано право читання документа.

Таким чином ідентифікація фізичної особи в інформаційно-комунікаційних системах здійснюється: з метою взаємодії з іншими особами (спілкування в соціальних мережах, на форумах тощо); для отримання доступу до інформації в мережі; для встановлення осіб, винних у вчиненні протиправних дій; з метою вступу в цивільні правовідносини та вчинення правочинів, та отримання державних послуг. Визнаючи потреби юридичної ідентифікації особи в цифровому середовищі, розвиток правового становища особи в цифровому середовищі характеризується транскордонним характером.

У залежності від вимог інформаційно-комунікаційної системи, може вимагатися встановлення всіх ідентифікуючих ознак особи, а в інших може вимагатися лише пред’явлення окремих ідентифікаторів.

Індивідуалізаційні ознаки або ідентифікатори (термін, який застосовується в актах ЄС, зокрема Регламенті ЄС 2016/679) набуваються особою за фактом народження, проходження процедури ідентифікації та реєстрації в мережі; містяться на паперових, електронних носіях, у реєстрах або можуть бути представлені в інших формах. При цьому незалежно від виду чи форми будь-яка ознака, що дозволяє ідентифікувати особу, насамперед є інформацією, використання якої сприяє встановленню ідентичності суб’єкта.

Банкам надається можливість обрання повноцінної моделі віддаленої ідентифікації та верифікації або спрощеної моделі, яка передбачає обмеження щодо обсягів проведення операції, та залишків за рахунками клієнтів. Так, до повноцінних систем верифікації та ідентифікації відноситься: ідентифікація за допомогою системи BankID та КЕП; відеоверифікація (спілкування клієнта та працівника банку через відеотрансляцію). До спрощених систем верифікації відноситься: ідентифікація за допомогою Системи BankID та КЕП; верифікація за допомогою КЕП; проведення платежу на окремий рахунок банку з особистого рахунку клієнта (із супроводженням його ПІБ); дистанційне зчитування даних з чипу документа який посвідчує особу за допомогою NFC модуля смартфона та мобільного додатка банку; верифікація даних з бюро кредитних історій (із отриманням повідомлення на телефон який підтверджує особу). Функціонування механізму BankID дозволяє отримати доступ до адміністративних та банківських послуг дистанційно. BankID залишається єдиною електронною системою верифікації фізичної особи, яка дозволяє підтвердити особу дистанційно та отримати доступ до адміністративних та банківських послуг) [191].

Р.Б. Шишка називає такі індивідуалізаційні ознаки: природнього походження (як біометричні дані – вік, стать, обличчя, папілярні лінії на пальцях (відбитки пальців), структура сітківки ока, генокод); побутові (зменшена назва, прізвисько, статус у сім'ї (батько, мати тощо), що спрощує спілкування та час на нього); психологічні (темперамент, почерк, підпис, наявність особливих здібностей психомоторної діяльності); територіальні (місце постійного або переважного проживання, місце перебування); соціальні (честь, репутація); формальні (відображені в офіційно виданих документах, посвідченнях особи); особисті (гідність, самооцінка, досвід юридично значущої діяльності, визнання як фахівця, пірсинг, татуювання); медичні; юридичні; публічні; комунікаційні; професійні (псевдоніми, вигадані імена), освітні, інше (релігійна приналежність); вікові (так, Всесвітньою організацією охорони здоров'я виділено: юні – до 18 років; молоді – від 18 до 44 років; середній вік – 45-59 років; літні – 60-74 роки; старечі – 75-90 років; довгожителі – більше 90 років). На

погляд науковця, під індивідуалізацією фізичної особи розуміється притаманні конкретній фізичній особі особисті ідентифікаційні ознаки, які відрізняють її з-поміж інших фізичних осіб та мають юридичне значення, уособлюють правовідношення або зумовлюють певні суб'єктивні права та юридичні обов'язки, які підлягають охороні та захисту у встановленому законом порядку[278, с. 565].

Також ознаки, які дозволяють ідентифікувати особу, можуть бути нерозривно пов'язані з нею, становити біологічні властивості, на підставі яких проводиться ідентифікація особи, як біометричні дані та дані, що набуваються впродовж життя, як ім'я, підпис (електронний, власноручний), коди, що присвоюються органами державної влади або учасниками цивільно-правових відносин та ін. Ознаки, що набуваються внаслідок інтелектуальної діяльності або створюються за допомогою використання технології уповноваженими органами або за договором. Так, О.А. Устименко пропонує впровадження критерію диференціації ознак, іманентних інституту індивідуалізації, в залежності від можливості їх зміни на: динамічні, які можуть бути трансформовані упродовж життя фізичної особи (ім'я, громадянство, родинний стан та ін.), та статичні, які не підлягають трансформації, в тому числі злочинним шляхом, до яких можна віднести біометричні дані особи (за виключенням відцифрованого підпису) [255].

Як зазначає Н.В. Волкова, залежно від ознак, індивідуалізувати людину можна трьома способами: формально (по імені, по батькові, прізвищу, місцю проживання і т. ін.), соціально (за зовнішнім виглядом, зв'язком з родичами та ін.) і правосуб'єктно (за наявності будь-яких ознак, що дають або не дають їй можливості брати участь у цивільних правовідносинах). У результаті трьох зазначених видів індивідуалізації, можна скласти три «портрети» громадянина: «формальний», «соціальний» і «правосуб'єктний», які можуть бути «намальовані» за допомогою засобів індивідуалізації, що є правовими засобами[26, с. 238].

Науковиця пропонує поділяти всі правові засоби індивідуалізації на приватноправові та публічно-правові. При цьому приватноправові засоби індивідуалізації фізичних осіб випливають із самої природи людини (включають цивільно-правові засоби індивідуалізації, тобто ті, що встановлені цивільним законодавством (ім'я, місце проживання, стани фізичної особи тощо), а публічно-правові – встановлюються державою і служать для відокремлення фізичної особи саме як учасника публічних правовідносин (наприклад, громадянство, ідентифікаційний код, місце реєстрації тощо).

Як нам уявляється, при визначенні правової ідентифікації суб'єктів у мережі «Інтернет» необхідно брати до уваги можливості конкретної ідентифікації особи та розділяти: ознаки, які допускають та не допускають конкретну ідентифікацію особи. Під неможливістю конкретної ідентифікації розуміється «ймовірнісна ідентифікація», яка на основі аналізу значного обсягу даних, за окремими ознаками не дозволяє ідентифікувати особу або у поєднанні з інформацією про поведінку (дії) особи, які через їх унікальність призводить до ідентифікації фізичної особи. Прикладом такої ймовірнісної або відносної ідентифікації можна навести ідентифікацію із застосуванням файлів кукі.

У залежності від обізнаності про результати ідентифікації для учасників правовідносин можна виділяти: абсолютну (по відношенню до всіх суб'єктів) та відносну (лише для ідентифікованої особи) ідентифікацію. Ідентифікація також може проводитись платно та безплатно. Так, системи ідентифікації для отримання державних послуг на державних платформах є безоплатними.

У науці висловлюється думка, що персональні дані становлять окрему групу індивідуалізуючої інформації про особу [268, с. 26]. Відповідно до даної позиції, означені категорії співвідносяться як ціле та частина, де будь-які персональні дані кваліфікуються як індивідуалізуюча інформація про фізичну особу, поряд з якими виокремлюється інша інформація, яка індивідуалізує особу та не відноситься до персональних даних.

Проте означена точка зору потребує уточнення в частині визначення персональних даних, з урахуванням аналізу Регламенту ЄС 2016/679. Розвиток

цифрового суспільства вносить свої неминучі трансформації, де обробка даних з одноразової дії перетворилася у майже безперервний процес. Суб'єкти даних подекуди не усвідомлюють масштаби даних, які збираються та обробляються щодо них, та факту такої обробки, коли втрачається межа між персональними та неперсональними даними [718].

З урахуванням євроінтеграційного шляху України, привертає увагу доктринальна та законодавча практика щодо тлумачення персональних даних (ідентифікаторів) в інформаційному суспільстві в ЄС. Відповідно до ч. 1 ст. Регламенту ЄС 2016/679 передбачено визначення персональних даних як будь-якої інформації, яка відноситься до суб'єкта даних, тобто ідентифікованої та підлягаючій ідентифікації фізичної особи; фізична особа, яка піддається ідентифікації – це особа, яку можна прямо або опосередковано ідентифікувати, зокрема за допомогою посилання на ідентифікатор, такий як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн- ідентифікатор, або на один, або декілька факторів, специфічних для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної ідентичності цієї фізичної особи.

Для з'ясування питання щодо співвідношення «персональних даних» та інформації про особу поряд із Регламентом необхідно звернутися до Позиції WP29 4/2007 Про концепцію персональних даних від 20.06.2007 (надалі Позиції WP29 4/2007) [708]. Відповідно до ст. 4 Регламенту ЄС 2016/679 персональними даними розуміється будь-яка інформацію, яка відноситься до ідентифікованої або фізичної особи, яка підлягає ідентифікації («суб'єкт даних»); ідентифікованою фізичною особою розуміється особа, яка може бути ідентифікована прямо або опосередковано, зокрема за допомогою посилання на ідентифікатор, такий як ім'я, прізвище, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або один, або декілька характерних для зазначеної особи фізичних, фізіологічних, генетичних, духовних, економічних, культурних факторів, або посилаючись на фактори соціальної ідентичності.

Відтак Регламент навмисно передбачає досить широке визначення персональних даних, яке не має чітко встановлених меж та єдиних критеріїв для того, щоб охопити максимально значну кількість даних. Первісний Проєкт Директиви 95/46/ЄС про захист фізичних осіб при обробці персональних даних та про обіг таких даних [492, с. 51], запропонований Комісією ЄС, передбачав застереження, що: визначення поняття персональних даних навмисно дається досить широким, аналогічно визначенню передбаченому Конвенцією Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних від 28 січня 1981 р. № 108 (Конвенція 108) [819], задля того, щоб охопити всі дані, які можуть бути пов'язані з особою. З цією позицією надалі погодився Європейський парламент, зазначивши, що визначення поняття «персональні дані» має бути якомога загальним, щоб охопити всю інформацію стосовно особи, яка ідентифікується. Ця позиція надалі була підтримана Радою ЄС та знайшла подальше відображення в судовій практиці ЄСПЛ.

Означений підхід відтворено в Керівних принципах щодо захисту конфіденційності та транскордонних потоків персональних даних Організації економічного співробітництва та розвитку 1980 року [696], Законі України Про захист персональних даних. Подібна норма міститься у ст. 4 Закону КНР про захист персональних даних від 20 серпня 2021 року [739].

ЄСПЛ виходить із того, що захист персональних даних охоплюється правом на повагу до приватного життя та гарантується ст. 8 ЄКПЛ. Адже ЄСПЛ визначає збір та обробку даних, що дозволяють ідентифікувати фізичну особу, як втручання у приватне життя [392]. ЄСПЛ відносить до персональних даних досить широке коло даних, що пов'язані з різними аспектами фізичної та соціальної ідентичності людини[395], зокрема ім'я, відомості про гендерну та етнічну приналежність, інтимні та сімейні сторони життя[372], здоров'я[416], зображення (фотографії)[415], зразки голосу[400], відбитки пальців, ДНК-профілі та клітинні зразки [408]. За таких умов, до категорії персональних даних відноситься досить широке коло даних [309, с. 13].

Широкий підхід до визначення персональних даних сформований у нормативно-правових актах ЄС, ефективно себе проявляє в ситуаціях періодичної обробки даних в межах встановленої процедури із чітко ідентифікованою особою (під час надсилання документів або заповнення анкет). Поряд із цим, в умовах розвитку цифрового суспільства розмежування між персональними та неперсональними даними поступово стирається [494, с. 323].

За твердженням М. Фінка та Ф. Паллас, аналіз положень Регламенту ЄС 2016/679 дозволяє дійти висновку, що в ЄС використовується підхід до правового регулювання обробки персональних даних, заснований на дихотомічній концепції розділення інформації та розмежування правових режимів обробки персональних та неперсональних даних. У межах даного підходу відповідні категорії виступають як додаткові категорії одна до одної, та виключають одна одну. Проявом такого виключення є те, що дані категорії сформульовані в законодавстві від зворотного, де персональні дані розуміються як будь-яка інформація, яка відноситься до ідентифікованої або фізичної особи, яка підлягає ідентифікації, у свою чергу, до неперсональних даних відносяться дані, за виключенням персональних.

Використання такого формулювання щодо визначення поняття неперсональних даних на його безпосередній зв’язок з персональними даними, свідчить про їх взаємозалежний або похідний характер. Означена позиція також відображається в науці, де міститься визначення неперсональних даних, засноване на розумінні персональних даних як будь-якої інформації, яка не відноситься до фізичної особи, коли така інформація не приводить прямо або опосередковано до ідентифікації.

Невід’ємним елементом встановлення приналежності інформації до категорії неперсональних даних є розуміння того, які саме дані належать до персональних. Тож одні й ті ж дані за певних обставин можуть як не визнаватися персональними даними, так і визнаватися такими, якщо за ними фізичну особу можна прямо або опосередковано ідентифікувати.

Європейська комісія проводить поділ неперсональних даних на два види залежно від походження інформації. Проте така класифікація, по суті, ґрунтується не лише на походженні інформації, а й відображає відмінність між відповідними видами неперсональних даних.

Перший вид виділяє інформацію, яка від початку не стосується фізичної особи. До таких неперсональних даних слід віднести метеорологічні, географічні, екологічні відомості, показники страхових та фінансових ринків, дані державної статистики, економічні та аналітичні показники тощо. Наприклад, дані про погодні умови, отримані за допомогою датчиків, встановлених на вітряках (вітрогенераторах). Другий вид об'єднує дані, які спочатку були персональними, але згодом відділені від особи та були анонімізовані. Видається, що до другого виду даних можуть бути включені анонімні дані, які від початку були відібрані таким способом, який не дозволяє ідентифікувати суб'єкта даних.

Розгляд Позиції Про концепцію персональних даних WP29 4/2007 дає підстави звернути увагу на такі складові елементи у конструкції визначення персональних даних, передбачені Регламентом ЄС 2016/679: «будь-яка інформація», «що стосується» «ідентифікованої особи або особи, яка підлягає ідентифікації», «фізичної особи». За допомогою цих елементів законодавець запровадив алгоритм виявлення та віднесення даних до персональних даних з-поміж решти оброблюваних даних. Необхідно брати до уваги, що в окремих випадках встановлення критеріїв розмежування персональних даних від неперсональних є досить неоднозначними, що може ускладнювати відмежування означених категорій у роботі контролера.

Регламент ЄС 2016/679 (П. 14 Преамбули) передбачає під суб'єктами даних виключно фізичних осіб, що автоматично призводить до того, що дані, які стосуються юридичних осіб, не визнаються персональними даними, що підтверджується Судом ЄС [370]. Проте Суд ЄС в рішенні по справі Volker und Markus Schecke GbR v. Land Hessen [586] зазначив, якщо офіційне найменування юридичної особи дозволяє ідентифікувати одну або декількох фізичних осіб

(коли назва компанії є ім'ям суб'єкта даних або декількох суб'єктів даних), у такому випадку юридична особа може вимагати захист права на недоторканність приватного життя та права на охорону персональних даних, закріплених у Хартії ЄС про основні права.

Крім того, інформація, що стосується померлих осіб, не вважається персональними даними, які підпадають під захист Регламенту ЄС 2016/679, оскільки померлі особи не розуміються як фізичні особи, носії прав та обов'язків. Однак у деяких випадках дані померлого все ж можуть отримати певний захист.

З іншого боку, інформація про померлих може стосуватися і живих осіб. Наприклад, інформація про те, що померла особа страждала на генетичну хворобу, яка передається спадкоємцям, вказує на те, що її діти також можуть нею страждати. Таким чином, інформація, яка є даними про померлих, може вважатися такою, що одночасно відноситься до живих і визнаватися персональними даними, що підпадають під дію Регламенту ЄС 2016/679. Такі персональні дані померлого, можуть опосередковано підпадати під положень про захист персональних даних.

При визначенні того, які дані відносяться до конкретної особи, необхідно брати до уваги кількісні та якісні характеристики отримуваних даних, такі як зміст, мета, для якої проводиться збір. Аналогічно зміст, мета та результат як елементи, кожен з яких незалежно від наявності інших, може зробити будь-яку інформацію такою, що «стосується» суб'єкта, називає Позиція WP29. Інформація може стосуватися суб'єкта за змістом, якщо вона про конкретну фізичну особу, наприклад, результати здачі іспиту, номер телефону конкретної особи, профіль певного користувача в соціальній мережі. Інформація може стосуватися суб'єкта за метою, якщо вона використовується або, найімовірніше, може бути використана з метою оцінки, впливу на статус або поведінку суб'єкта, прояву певного відношення до суб'єкта.

Наприклад, відвідування сторінок в інтернеті співробітниками компанії може бути використано для моніторингу ефективності впродовж робочого часу або з метою обмеження доступу до певних сторінок. Інформація може

стосуватися суб'єкта персональних даних, навіть за відсутності ознаки «змісту» та «мети», якщо є ознака результату: якщо обробка даних із високою ймовірністю може вплинути на права та інтереси суб'єктів даних. У випадку зміни ставлення оточуючих до особи, якщо дані призведуть до виокремлення особи у колі її співробітників та друзів. Наприклад, інформація про родичів школяра, які отримали нагороду Праведник народів світу, може призвести до глузування та знущання з боку однолітків. Ці три елементи відношення даних до суб'єкта застосовуються кожен окремо, але, якщо є хоча б один елемент, немає необхідності виявляти інші два – дані визнаються такими, що відносяться до суб'єкта.

Тому при встановленні, чи відносяться дані до неперсональних, необхідно брати до уваги, чи можна визнати за правом ЄС дані про об'єкт до персональних даних за умови, якщо такі дані дозволяють ідентифікувати суб'єкта даних [240, с. 169].

Третім елементом, який покликаний встановити, чи відносяться дані до персональних даних є ті, що стосуються «ідентифікованої або фізичної особи, яка підлягає ідентифікації». Означене має кваліфікуюче значення для номерів телефонів та інших номерів, характеристик об'єктів, живих істот (тварин), які стосуються суб'єкта даних.

Позиція WP29 визначає особу як таку, що підлягає ідентифікації, якщо вона ще не ідентифікована, але її можна ідентифікувати безпосередньо, наприклад, за ім'ям (якщо воно дозволяє виокремити суб'єкта з-поміж інших) або опосередковано – за номером паспорта, автотранспортного засобу, телефону або комбінації істотних ознак, що дозволяють виокремити суб'єкта (за віком, місцем проживання, зовнішнім виглядом тощо).

Дані, «які відносяться до» фізичної особи, включають не лише інформацію про самого суб'єкта даних, але й про належні йому або пов'язані з ним об'єкти. Наприклад, домашніх тварин та характеристики цих об'єктів, такі як вартість, стан зношення, серійний номер, діагноз, результати аналізів та обстежень тощо. Так, в окремих випадках інформація, що стосується об'єкта, може

опосередковано бути джерелом інформації про особу. Вартість транспортного засобу є даними про об’єкт, а інформація про сплату транспортного податку власником зазначеного транспорту може визнаватися як персональні дані [708]. Дані можуть як безпосередньо стосуватися фізичної особи (ім’я, ДНК, чіп біометричного паспорта, RFID-мітка), так і опосередковано (наприклад, дані телефонних дзвінків на роботі), або можуть залежно від їх використання породжувати наслідки для фізичної особи (наприклад, GPS-дані у службових автотранспортних засобів).

Водночас вірогідна або гіпотетична ймовірність ідентифікації суб’єкта не робить автоматично інформацію персональними даними. Якщо можливість ідентифікувати суб’єкта відсутня або досить низька, такі дані не будуть визнаватися персональними даними. Зазначена теза, на думку розробників Позиції WP29, може бути використана контролером як маніпуляція та виправдання збору персональних даних, яке не мало наміру ідентифікувати особу, персональні дані якої збираються. Проте за номерами телефонів, автотранспортних засобів, карток, особу можна ідентифікувати у випадку порівняння цих даних із даними з інших баз, наприклад, у випадку міжвідомчого обміну даними, отримання даних від операторів мобільного зв’язку, камер відеоспостереження на вулиці.

Щодо питання кваліфікації номера телефону як ідентифікатора та визнання його персональними даними, то в кожному конкретному випадку необхідно визначати наявні можливості та необхідні ресурси, які мають бути додані контролером для ідентифікації суб’єкта за номером телефону. Якщо можливість є, або мета та контекст обробки передбачає ідентифікацію суб’єкта, номер телефону буде виступати як персональні дані. Дане правило має за аналогією застосуватися і до інших номерів.

Регламент та Позиція WP29 виходить з того, що у разі відсутності даних про прізвище, ім’я та по батькові суб’єкта персональних даних та неможливості ідентифікувати суб’єкта, контролер та третя особа ладні істотно вплинути на

поведінку суб’єкта, порушивши його права та інтереси в інтернеті за наявності в них лише телефонного номера.

Характерною особливістю номера телефону, яка відрізняє його від інших номерів, речей, є можливість безпосереднього зв’язку з суб’єктом та істотного втручання у приватне життя, завдання шкоди здоров’ю. Наприклад: шахрайство, телефонні дзвінки у вечірній час доби, настирливі повідомлення можуть змусити суб’єкта змінити номер телефону, та змінити контролера, з вини якого відбулося порушення його прав. Загалом контактні дані (номер телефону, адреса електронної пошти, домашня адреса тощо) дозволяють шахраям безпосередньо зв’язатися із суб’єктом даних попри його волю, загрожуючи його життю та безпеці, маніпулюючи, втручаючись у приватне життя.

Позиція WP29 дотримується ідеї, що за наявності контактних даних третьої особи, може призвести до порушення його права, навіть якщо суб’єкт не може бути ідентифікований. Конфіденційність цих даних забезпечує безпеку життя та здоров’я суб’єкта, його близьких, дозволяє контролювати зовнішню комунікацію, знижує його доступність для зовнішнього світу, вибудовує особисті межі суб’єкта, оберігає його особистий простір, що дає суб’єкту комфорт та впевненість [708].

Позиція WP29 бере до уваги те, що для визначення ступеня вірогідності та ймовірності того, що контролер або інша третя особа, яка заволоділа інформацією, спробує ідентифікувати суб’єкта за такими даними, слід брати до уваги, які розумні зусилля контролер або будь-яка третя особа мають докласти, щоб ідентифікувати конкретного суб’єкта: витрати грошових коштів та зусиль; людських ресурсів; існування технології, що дозволяє виконати ідентифікацію без додаткових зусиль та витрат; поставлена мета, а не декларована; які переваги може отримати контролер або інша особа; тривалість зберігання даних та потенційний розвиток технологій для ідентифікації в означений проміжок часу. Тож необхідно брати до уваги всі об'єктивні чинники, такі як фінансові та часові витрати, необхідні для проведення ідентифікації, рівень технологій та їх доступність для суб’єктів у момент обробки даних. Такий алгоритм обробки

персональних даних ґрунтується на оцінці ризику ідентифікації суб'єкта, а не на можливості ідентифікації особи як такої. Отже, за даним підходом інформація, яка є персональною, може бути визнана неперсональними даними у випадку, якщо ідентифікація особи за її допомогою невигідна або недоцільна, оскільки потребує непропорційно великих витрат.

М. Фінк та Ф. Паллас звертають увагу на те, що позиція Європейської ради з захисту даних, у частині визнання неперсональними даними тільки тієї інформації про фізичну особи, яка за жодних обставин не дозволяє ідентифікувати особу, є вочевидь поширюваною. Науковці застерігають щодо занадто широкого тлумачення та динамічність розуміння категорії персональні дані, передбаченої Регламентом 2016/679 [516, с. 11]. Підхід, викладений у Регламенті в умовах стрімкого розвитку інформаційно-комунікаційних технологій уявляється більш ефективним у порівняні з абсолютним підходом, якого дотримується Європейська ради з захисту даних.

Поряд із персональними даними необхідно назвати псевдонімізовані та анімізовані дані. Анонімізовані дані є такими даними, які не дозволяють провести ідентифікацію особи, не підлягають захисту як персональні дані та не захищаються законодавством про захист персональних даних, зокрема Регламентом 2016/679. Псевдонімізація передбачає обробку персональних даних у такий спосіб, що не дозволяє більше віднести дані до певного суб'єкта без використання додаткової інформації за умови, що додаткова інформація зберігається окремо та підпадає під технічні та організаційні заходи, які гарантують, що персональні дані не можна буде співвіднести з фізичною особою (п. 5 ст. 4 Регламенту 2016/679). Керівництво з регулювання вільного руху неперсональних даних в ЄС зазначає, що провідна відмінність псевдонімізованих та анонімізованих даних полягає в тому, що дані, анонімізовані належним чином, навіть за наявності додаткових даних не можуть знову стати персональними [720]. М. Фінк та Ф. Паллас стверджують, що з урахуванням сучасного рівня розвитку інформаційно-комунікаційних

технологій та науково-технічного розвитку, після проведення процедури анонімізації даних залишається вірогідність ідентифікації суб'єкта [516, с. 11].

Можна стверджувати, що масштаби обробки даних та науково- технічний розвиток вплинули на підхід до визначення персональних даних. Привертає увагу аналіз тлумачення категорії «рівень науково-технічного розвитку» або «рівень розвитку» (state of art) з огляду на значущість для інформаційної приватності та захисту персональних даних. Керівництво з регулювання вільного руху неперсональних даних в ЄС (п. 18, 20, 21, 22) зазначає, що поняття «рівень науково-технічного розвитку» міститься в різних актах ЄС, наприклад, у сфері охорони довкілля та безпеки продукції [720]. Органи нагляду за захистом даних, такі як британський Офіс Інформаційного комісару [293] та CNIL, посилаються на дану категорію у правилах та керівних принципах безпеки даних. Поряд із тим, не містять визначення. У Регламенті 2016/679 посилання на «рівень науково-технічного розвитку» міститься у ст. 32 (щодо заходів безпеки, які має впроваджувати контролер даних) та ст. 25 (щодо обов'язку контролера вживати заходи вбудованої приватності та за замовчуванням). Аналіз ст. 25 та 32 Регламенту 2016/679 дозволяє дійти висновку, що дану категорію необхідно застосовувати до всіх технічних та організаційних заходів обробки даних. Розуміння категорії «рівень науково-технічного розвитку» міститься в рішенні Федерального конституційного суду Німеччини у справі «Калкар» 1978 року. Відповідно до тлумачення, даного Судом, «рівень науково-технічного розвитку» розуміється між технологічним рівнем «наявних наукових знань та досліджень» та більш усталених «загальноприйнятих правил». Отже, «рівень науково-технічного прогресу» може розумітися як технологічний рівень послуги, технології або продукту, представленого на ринку та є найбільш ефективним для досягнення поставленої мети [391]. Керівництво зазначає, що «рівень науково-технічного розвитку» є динамічною категорією, яка не може бути визначена в певний проміжок часу та потребує постійного оцінювання контролером з урахування бурхливого розвитку технологій. Завдяки невпинному розвитку технологій, контролер може виявити, що ті заходи безпеки, які він раніше

застосовував для забезпечення належного рівня захисту, не відповідають вимогам належної безпеки. Ігнорування розвитку технологій та змін у галузі безпеки може призвести до порушення прав суб'єктів та недотримання ст. 25 Регламенту 2016/679. Критерій «рівень науково-технічного розвитку» може бути застосований не лише до технологічних заходів, а й до організаційних. Відсутність необхідних організаційних заходів може нівелювати ефективність застосування технології. Прикладами організаційних заходів можуть бути: прийняття внутрішніх правил, підвищення кваліфікації та навчання працівників компанії в галузі інформаційної безпеки та захисту персональних даних; управління інформаційною безпекою. Існуючі та визнані стандарти, сертифікації, кодекси поведінки тощо в різних галузях можуть зіграти роль у визначенні поточного «рівня науково-технічного розвитку» в межах цієї галузі. Там, де такі стандарти існують і забезпечують високий рівень захисту суб'єкта даних відповідно до правових вимог або перевершують їх, контролери повинні враховувати їх при розробці та реалізації заходів щодо захисту даних. Можна стверджувати, що «рівень науково-технічного розвитку» стає орієнтиром, який контролери змушені постійно брати до уваги з моменту розробки та функціонування товару (послуги).

Підсумовуючи викладене слід зазначити, що питання удосконалення засобів ідентифікації нерозривно пов'язано з проблемою втручання в недоторканність приватного життя, зростанням обсягів персональних даних, які збираються. Будь-які рішення щодо збору додаткових даних та ідентифікації суб'єкта має вирішуватися з урахуванням інтересів фізичної особи, недопущенням втручання у приватне життя.

2.4. Ідентифікуючі ознаки фізичної особи у відносинах у мережі «Інтернет»

Рівень формальної індивідуалізації відносин в мережі «Інтернет» може варіюватися. Ступінь формалізації може залежати від характеру цивільних відносин та відповідно впливати та обсяг ідентифікаторів, необхідних для вступу в ці відносини та набуття прав та обов'язків. Індивідуалізуючі засоби суб'єктів, які широко використовуються та однозначно сприймаються у традиційних правовідносинах, можуть набувати дещо іншого значення у віртуальному середовищі.

Фізична особа набуває і здійснює належні йому права та обов'язки під своїм ім'ям, яке супроводжує її все життя (якщо не відбудеться його зміна). А зміна особою свого імені не є підставою для припинення або зміни її прав та обов'язків, набутих під колишнім іменем, особа зобов'язана у цьому випадку вжити необхідні заходи для повідомлення своїх боржників і кредиторів про зміну імені. Невиконання зазначеного обов'язку покладає на нього ризик наслідків, спричинених відсутністю в зазначених осіб відомостей про зміну його імені. Ім'я особи є традиційним індивідуалізуючим засобом, який вирізняє її від інших та пов'язує із собою всю сукупність уявлень про внутрішні та зовнішні якості носія. Згідно зі ст. 294 ЦК України передбачено, що фізична особа має право на ім'я. Ім'я фізичної особи, яка є громадянином України, складається із прізвища, власного імені та по батькові, якщо інше не випливає із закону або звичаю національної меншини, до якої вона належить. Ім'я фізичній особі надається відповідно до закону (ст. 28. ЦК України).

З.В. Ромовська зазначає, що зміст права людини на ім'я складається насамперед з таких елементів як: право бути названою; право називатися іншими так само, як нарекли батьки; противитися будь-яким спробам переінакшити надане батьками ім'я; право на звернення до відповідних органів із заявою про зміну наданого батьками імені [187, с. 330].

Право на індивідуальність фізичної особи – це суб'єктивне особисте немайнове право, яке полягає в можливості формувати та використовувати

індивідуальні ознаки, сукупність яких становить особливість фізичної особи, що робить її своєрідною та впізнаваною серед інших осіб. Фізична особа володіє комплексом особистих немайнових прав, що забезпечують не тільки соціальне буття фізичної особи, а й ті, що забезпечують природнє існування фізичної особи [32, с. 37].

Правове регулювання права на ім'я пов'язується із моментом народження. Відповідно до п. 2 ст. 24 МПГПП передбачено, що кожна дитина має бути зареєстрована негайно після народження та отримати ім'я.

Право на ім'я реалізується громадянином у процесі цивільного обороту, зокрема під час вчинення правочинів, підписання договорів, за допомогою власноручного підпису або використання його аналогів – електронного.

Використання псевдоніму, сценічного імені та творчого прізвиська, умовного імені має місце в галузі науки, літератури, мистецтва та журналістики (ст. 438 ЦК України та ст. 9, 11 Закону України «Про авторське право та суміжні права»[144], ст. 25 Закону України «Про інформацію») [159]. Щодо нікнейму в інтернеті, то він може прирівнюватися до псевдоніму [21]. Поряд із цим, використання нікнейму в мережі може бути обмежено вимогами користувацьких угод. У КНР обмеження використання вигаданих імен або псевдонімів обмежується державними приписами.

Відтак ідея анонімності у віртуальному просторі є не новою, оскільки являє собою модифікацію проблеми використання фізичною особою псевдоніму. Цивілістика не заперечує можливості використання вигаданого імені. Фізичній особі належить право використовувати псевдонім, коли вона вважає за необхідне (за умови, що використання такого псевдоніму не є зловживанням правом і не має на меті навмисне введення в оману щодо особи носія псевдоніма). Охороняючи псевдонім, держава забезпечує охорону прав та інтересів фізичної особи та проявів людської особистості.

Водночас правила користувацьких угод можуть містити обмеження на зміну імені користувача. Так, TikTok містить обмеження та допускає використання лише літер, цифр, підкреслень та точок в імені та дозволяє зміну

імені один раз на 30 днів. TikTok надає право користувачам створювати пародійні акаунти для творчого самовираження поряд із основним акаунтом, водночас не допускається створення акаунтів із метою введення в оману користувачів[253]. Facebook передбачає використання справжніх імен, обумовлюючи спілкування з реальними людьми та захистом спільноти від спроб видати себе за іншу людину, шахрайства та фішингу. Обмеження стосуються зміни імені протягом 60 днів, якщо використання імен порушує правила спільноти або створення фейкових акаунтів. Обмежується використання як імені: символів, цифр, повторюваних символів або розділових знаків; символів із різних мов; звань як імені (наприклад, професійних або релігійних); слів або фраз замість імені; образливих або непристойних слів та виразів. У випадку втрати доступу до акаунту, неможливості відновити реєстраційні дані Facebook може запросити посвідчення особи державного зразка або інші недержавні документи, де фото, ім’я, дата народження співпадає із даними профілю [85].

Спочатку використання псевдонімів в інтернеті було обумовлено можливістю вступати у відносини із дотриманням умов анонімності та приватності. Водночас переваги використання псевдоніму зменшуються не лише через зміну цінностей у мережі, а й через те, що псевдонім не виключає ймовірність відстеження особи за ним. Тому К. Кумаяма говорить про «право не бути відстеженим» у мережі, яке будучи юридично забезпеченим, має мінімізувати фактичну ймовірність відстеження, надаючи особам захист псевдонімів, право на певну суму компенсації. З погляду науковця, право не бути відстеженим випливає з трьох різних відносин і прав. По-перше, з фідуціарних відносин між користувачем та постачальником. Якщо персональні дані користувача з необережності постачальника ідентифікаційних даних будуть розкриті, то користувач буде скомпрометований. Для запобігання такій недбалості мають бути передбачені як законодавчі, так і компенсаційні механізми відшкодування збитків користувачеві. По-друге, ці відносини довіри між користувачами та державними органами повинен мати можливість відстежувати профіль, представлений псевдонімом для забезпечення

дотримання законодавства в разі вчинення ним порушень. Але для дотримання приватності та забезпечення переваг псевдонімів, державні органи мають дотримуватися засад приватності та не порушувати завісу псевдонімів без дотримання належної правової процедури. Так, чотирнадцята поправка Конституції США гарантує заборону на обмеження прав інакше як за рішенням суду [606, с. 428]. На думку К. Денбі, дотримання засад приватності та «права не бути відстеженим» має забезпечити здійснення права на свободу вираження в мережі без побоювання переслідування, зокрема в репресивних режимах [474]. Третій аспект має значення в практиці США. Перша поправка Конституції США охороняє право людини говорити правду про інших, за виключенням деяких ситуацій. Як наслідок, користувач, який повідомив про існування профілю під псевдонімом, як правило не повинен мати жодних засобів правового захисту, якщо особа розкриває цю інформацію іншим. Виключенням є ситуація, коли фізична або юридична особа, яка отримала інформацію шляхом введення в оману, або розголошує таку інформацію з метою отримання прибутку, може бути притягнута до відповідальності за її розголошення[606, с. 429].

К. Кумаяма дискутує з питання, чи має законодавство визнавати за особами, які діють під псевдонімом в мережі, право подавати позови до суду. Професори Р. Девід та Д. Пост стверджують, що особам, які діють під псевдонімом, слід надати право подавати позови, оскільки такий псевдонім може бути спаплюжено. У випадку визнання за такою особою повного кола права, вони можуть отримати економічну цінність, цінність торговельних марок та можливість ставати об’єктом договору купівлі-продажу. Право на відшкодування шкоди, завданої репутації мережевій особі, може бути обґрунтованою, навіть якщо ця особистість не відповідає в точності особистості особи у фізичному світі. З урахуванням практики США, у разі набуття популярності профілю під псевдонімом, особа може, вимагати правовий захист відповідно до законодавства про інтелектуальну власність, вимагати заборони використання псевдоніму в тій же сфері діяльності, де діє конкурент, через

введення в оману споживачів, вимагати заборони створювати конкуруючий блог та захисту репутації псевдоніму[606, с. 430; 459, с.1368].

Окремо слід назвати такий ідентифікатор фізичної особи як електронна пошта, який індивідуалізує фізичну особу в мережі «Інтернет» [268, с. 27]. Електронна пошта вказується при поданні заяв, офіційних документах, під час реєстрації акаунтів у державних та приватних інформаційно-комунікаційних системах.

Ідентифікуючою функцією особи також служить її зображення, яке може набувати різних виглядів та бути сконструйовано за допомогою технологій у мережі [207, с. 44]. Є.О. Мічурін звертає увагу, що індивідуалізацією фізичної особи в мережі «Інтернет» може служити не лише справжнє фото та відеозображення, а також анімація та зображення особи, створені з застосуванням цифрових інструментів[107, с. 91].

За загальним правилом, користування мережею «Інтернет» здійснюється відносно анонімно. Водночас законодавство може містити вимоги про неприпустимість анонімних відносин із держаними органами. Так, відповідно до ч. 1 ст. 8 Закону України «Про звернення громадян», письмове звернення без зазначення місця проживання, не підписане автором (авторами), а також таке, з якого неможливо встановити авторство, визнається анонімним і розгляду не підлягає. Такий підхід вважається виправдним та стосується таких випадків звернення до державних органів на електронні поштові адреси.

Кожне обладнання, доступне в мережі «Інтернет», у тому числі й те, що міститься на веб-сайтах, фізично розміщене на комп'ютерному обладнанні, об'єднаному каналами зв'язку з цією мережею, має IP-адресу. IP-адреса – є ідентифікатор, унікальний номер, який складається з набору чотирьох 8-бітних чисел, що використовується для адресації комп'ютерів у електронній мережі [267, с. 353].

Інформаційний центр з електронної приватності дотримується підходу, за яким IP-адреса розглядається як частина даних про трафік, що цифрова адреса пристрою, виражена у форматі, вказаному в інтернет-протоколі. IP-адреса являє

собою 32-бітну послідовність, розділену на чотири групи десяткових чисел, розділених періодами. У деяких випадках IP-адреса ідентифікує унікальний пристрій (комп'ютер, планшет, телефон тощо), в інших випадках, наприклад, коли мережа комп'ютерів підключається до інтернету через одне інтернет-з'єднання, може не ідентифікувати. IP-адреса комп'ютера певною мірою аналогічна телефонному номеру [746].

Потреба ідентифікації особи в мережі може бути обумовлена вчиненням правопорушення, коли майже єдиним засобом ідентифікації залишається IP-адреса. Крім того, процес встановлення порушників може бути ускладнений через використання технічних засобів, програм, які забезпечують повну анонімність та ускладнюють процес ідентифікації злочинця в мережі «Інтернет».

Відносно ідентифікації користувачів інтернету за IP-адресою, то слід звернути увагу, що ЄСПЛ у справі Benedik v. Slovenia [371] зробив висновок, що ідентифікація користувачів інтернету за IP-адресою є елементом приватного життя та порушує ст. 8 Конвенції про захист прав людини та основоположних свобод, про те, що органи державної влади не можуть втручатися у здійснення прав на повагу до приватного й сімейного життя, за виключенням випадків, коли втручання здійснюється згідно з законом[59]. Заявник стверджував, що поліція незаконно отримала інформацію від інтернет-провайдера про розкриття його персони через ідентифікацію по IP-адресі. Правоохоронні органи Швейцарії провели моніторинг користувачів мережі Razorback, під час якого поліція встановила, що деякі користувачі обмінювалися порнографічними відео та світлинами через мережу. На підставі розслідування, поліція подала запит до інтернет-провайдера з вимогою розкрити дані про користувача за його IP-адресою. Інтернет-провайдер, незважаючи на відсутність судового дозволу, надав правоохоронцям дані свого клієнта. На підставі цих даних суд визнав заявника винним у розповсюдженні порнографії та присудив 8 місяців умовного ув'язнення з випробувальним терміном у два роки. У скарзі до ЄСПЛ заявник зауважив, що провайдер зберігав його персональні дані незаконно, а поліція отримала персональні дані абонента без судового рішення в порушення статті 8

Конвенції. Суд погодився з позицією заявника, що захист його персональних даних в інтернеті підпадає під поняття «приватне життя» та встановив факт порушення статті 8 Конвенції. Суд також встановив, що запит поліції до провайдера щодо розкриття інформації про абонента порушив право на повагу до приватного життя. Заявник вимагав компенсацію завданої йому моральної шкоди в сумі 32 тис. євро, проте Суд постановив відшкодувати заявнику лише судові витрати на суму 3,5 тис. євро, вважаючи, що сам висновок про встановлення порушення є достатнім для задоволення моральної шкоди [371].

У разі визнання IP-адреси та інших даних мережевого трафіку, якими щодня обмінюються довірені особи в мережі як персональними даними, обробка цих даних буде вимагати дотримання законодавства про захист персональних даних.

Вищевказане є дискусійним, оскільки в разі такого визнання, на інтернет-провайдерів, пошукові системи будуть покладатися додаткові обов'язки дотримання суворих стандартів законодавства при зборі, обробці та захисту цих даних як персональних. Доволі консервативної думки щодо розгляду IP-адреси та даних про трафік як персональних даних дотримується Європейський наглядовий із захисту даних (EDPS), Робоча група 29 та комісари з даних [867].

З погляду Інспектора із захисту даних Європейського Союзу, особа не повинна бути обов'язково ідентифікована за іменем, щоб закон про захист даних міг застосовуватися до деталей використання комп'ютера. Інспектор заявив, що компанія, якщо має сумніви, повинна розглядати як персональні дані всю діяльність користувачів, у тому числі журнали про сервери та записи IP-адрес. Інспектор із захисту даних також зазначив, що для визнання IP-адрес як персональних даних, компанії, яка обробляє дані суб'єкта, не обов'язково має володіти додатковими даними як ім'я, дата народження, геолокація тощо. Натомість суб'єкта можна ідентифікувати під час виокремлення. У свою чергу, відстеження діяльності та поведінки суб'єктів за їх IP-адресою дозволяє виокремити їх таким чином, щоб конкретно ідентифікувати [845].

Разом з цим, з погляду Е. Тікка, слід розрізняти обробку даних з метою моніторингу та обробку даних з метою ідентифікації користувача за IP-адресою[827, с. 25]. Визначальним для встановлення того, чи виступає IP-адреса ідентифікатором та захищається законодавством про захист персональних даних, має відігравати не природа IP-адреси як така, а мета обробки. IP-адреса може виступати як персональні дані у випадку використання для встановлення особи правопорушника, водночас IP-адреса не виступає ідентифікатором, якщо метою обробки не є ідентифікація особи (що є основним завданням законодавства про захист персональних даних), а обробка даних проводиться з метою виявлення загроз, вразливостей і потенційних засобів захисту, управління мережами, моніторинг трафіку та обміну інформацією про аномалії.

Тож коли IP-адреса та інші дані про трафік обробляються з метою ідентифікації осіб правопорушників, у діяльності правоохоронних органів така обробка даних підпадає під дію законодавства про персональні дані, але обробки цих даних без мети ідентифікації суб'єкта даних, не дозволяє кваліфікувати їх як персональні дані.

У науці висловлюється точка зору, що для індивідуалізації суб'єкта слід закріпити в законодавстві можливість використання технічних методів (пристроїв і програмних засобів) для визначення належності учасника правовідносин до певної держави. Водночас слід брати до уваги п. 5 ст. 6 «Конвенції ООН про використання електронних повідомлень у міжнародних договорах» не створює презумпції знаходження комерційного підприємства в країні за фактом використання суб'єктом доменного імені або адреси електронної пошти, пов'язаної з конкретною державою [722].

Наступним поширеним та доступним засобом індивідуалізації в мережі «Інтернет» є доменні імена. Права на доменне ім'я може належати лише одній особі. Відповідно до ст. 1 Закону України «Про охорону прав на знаки для товарів і послуг», доменне ім'я – це ім'я, яке використовується для адресації комп'ютерів і ресурсів в інтернеті. Поняття домену міститься у п. 22 ст. 2 Закону України «Про електронні комунікації» [153], домен є частиною ієрархічного

адресного простору мережі «Інтернет», що має унікальну назву (доменне ім'я), яке її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється. Головною метою домену є ідентифікація та адресація веб-сайту в мережі «Інтернет», що реалізується завдяки системі доменних імен, яка являє собою розподільчий механізм перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу [93, с. 94]. Закон України «Про телекомунікації», який втратив чинність 01.01.2022, розрізняв домени верхнього та другого рівня нижчих рівнів; Домен.UA є доменами верхнього рівня ієрархічного адресного простору мережі «Інтернет», створених на основі кодування назв країн відповідно до міжнародних стандартів для обслуговування адресного простору українського сегмента мережі «Інтернет». Домени другого рівня – є частиною адресного простору мережі «Інтернет», що розташовується на другому рівні ієрархії імен у мережі.

Доменне ім'я розглядається в науці як об'єкт права інтелектуальної власності, доводиться цінність та оборотоздатність як об'єкта цивільних прав [114, с. 40] та як засобу індивідуалізації учасників відносин.

Доменне ім'я, будучи засобом індивідуалізації суб'єктів господарювання, а також некомерційних юридичних та фізичних осіб у мережі, зазвичай належать підприємницьким структурам, які використовують для популяризації та просування товарів та послуг. Відтак доменне ім'я володіє економічною цінністю для його власника. Доменне ім'я асоціюється із відомістю та репутацією особи, яка стоїть за інформаційним ресурсом [209].

За визначенням О.О. Кулініч, доменне ім'я є засобом ідентифікації певного інформаційного ресурсу в мережі «Інтернет», який за певних умов є похідним засобом індивідуалізації фізичних та юридичних осіб у мережі [91, с. 195]. Науковиця дотримується позиції, що доменне ім'я як позначення, призначене, в першу чергу, для індивідуалізації інформаційних ресурсів у мережі «Інтернет», індивідуалізація інших об'єктів та суб'єктів може здійснюватися, але лише як вторинна функція.

Серед провідних функцій доменного імені Н. Майданик називає ідентифікацію ресурсів у мережі «Інтернет» та забезпечення адресації в мережі[98]. На погляд О.М. Коршакова, функції доменних імен є значно ширшими та виконують асоціативну функцію щодо власників ресурсів, характеризуючи їх діяльність, авторитет та репутацію, надаючи можливість легкого пошуку його в мережі «Інтернет» серед аналогічних інформаційних ресурсів[94, с. 52].

Подекуди охорона комбінації літер, які складають доменне ім'я, забезпечується за допомогою реєстрації доменного імені як торговельної марки, яка за ст. 492. ЦК України визначається як будь-які позначення або будь-яка комбінація позначень, які придатні для вирізнення товарів (послуг), що виробляються (надаються) однією особою, від товарів (послуг), що виробляються (надаються) іншими особами. Такими позначеннями можуть бути: слова, літери, цифри, зображувальні елементи та комбінація кольорів.

Слід звернути увагу, що науковці Д. Жуванов, М.В. Петрів наголошують про необхідність відмежовувати доменні імена від торговельної марки та неприпустимість їх ототожнення. Серед відмінностей слід назвати те, що товарні знаки мають територіальні межі дії; реєструються за певними групами товарів; служать для ідентифікації товаровиробників певних товарів, послуг; як товарний знак можуть використовуватися будь-які позначення, комбінація позначень, у тому числі власні імена, алфавітні та цифрові послідовності, зображувальні елементи, кольори та їх комбінація. Також доменні імена носять екстериторіальний характер, не залежать від держави, де були зареєстровані; не призначені для орієнтування споживача на ринку товарів, робіт та послуг; як доменне ім'я можуть використовуватися алфавітні та цифрові послідовності [61; 128, с. 92].

Серед засобів ідентифікації фізичних осіб у мережі використовують кукі-файли. Оператори вебсайтів прагнуть збирати якомога більше персональних даних, відстежувати дії користувачів для підвищення персоналізації використання платформ, для чого їм необхідна юридична підстава, згода

суб'єкта даних на обробку персональних даних та використання файлів кукі, пікселів тощо. Кукі-файли використовуються для отримання згоди на збір та обробку даних про перебування та відстеження вчинків користувачів.

Файли кукі являють собою невеликі текстові файли, що розміщуються на комп'ютері (або смартфоні) користувача, які можуть використовуватися для збору персональних даних. Більшість сайтів розміщують файли cookie у браузері або на жорсткому диску комп'ютера користувача. Файли cookie можуть збирати інформацію про використання сайту або дозволяти вебсайту розпізнавати користувача як існуючого клієнта, коли він повернеться на вебсайт пізніше. Цей файл не є ні вірусом, ні шпигунським програмним забезпеченням. Законодавство захищає користувачів вебсайту та дозволяє їм відмовитися від використання файлів cookie у браузері вебсайту.

На практиці постає питання щодо можливості віднесення кукі-файлів до персональних даних та ідентифікаторів фізичної особи. Наприклад, до кукі-файлів, які збирають персональні дані, відносяться всі кукі-файли, які обробляють персональні дані: ПІБ, адреса, електронна пошта тощо. Таке використання є обробкою персональних даних, яке вимагає отримання згоди та проводиться відповідно до вимог законодавства про захист персональних даних.

Прикладом використання кукі-файлів є таргетована реклама, тобто персоналізована реклама, сформована з огляду на запити користувача. Наприклад, ввівши в пошуку запит, пов'язаний з купівлею будь-якої речі, ще через кілька днів рекламні оголошення рекламуватимуть подібну річ, це і є таргетована реклама, яка використовує ваші cookie-файли. Аналогічна ситуація може статися, якщо не відключена в додатку можливість використання мікрофона при вимкненому телефоні і тоді, якщо з телефоном, що лежить на столі, обговорюєте покупку якоїсь речі, навіть не вводячи нічого в пошукові системи, рекламні оголошення також з високою ймовірністю будуть показувати той об'єкт, який обговорювався.

Можна виділити такі види кукі-файлів: тимчасові, постійні, основні, сторонні, кукі-зомбі та флешкукі[481].

Тимчасові файли кукі або сеансові, які допомагають сайтам розпізнавати користувачів за інформацію, що надається при навігації по вебсайту та зберігають інформацію про дії користувача, доки він перебуває на вебсайті. Після закриття браузера видаляються, зазвичай використовуються на сайтах електронної комерції.

Постійні файли кукі – найбільш об'ємні, продовжують функціонувати після закриття веббраузера, подекуди використовуються рекламними сервісами, містять авторизовані дані користувачів для входу до облікового запису, щоб користувачу не доводилося вводити їх повторно кожного разу при вході.

Первинні файли встановлюються безпосередньо сайтом (тобто доменом), який відвідує користувач (тобто URL-адресою, яка відображається в адресному рядку браузера). Ці файли cookie дозволяють власникам сайтів збирати аналітичні дані, запам'ятовувати налаштування мови та виконувати інші корисні функції, які забезпечують зручність використання сервісами.

Сторонні кукі-файли встановлюються третіми особами з метою збирання певної інформації від користувачів для проведення досліджень як поведінки, споживацьких звичок. Не зберігаються на сайті користувача, а на сторонніх серверах, використовуються сторонніми рекламними серверами для збереження рекламних банерів та аналітичних скриптів (збирають інформацію, з якого сайту зайшов користувач, на якій частині сторінки користувач зупинився, на якій частині сторінки провів більше часу, який час загалом провів на сторінці тощо).

Флешкукі або суперкукі не залежать від веббраузера, постійно зберігаються на комп'ютері користувача навіть після того, як всі файли cookie були видалені з веббраузера. Функціонують в інтересах рекламодавця, третьої зацікавленої особи, відстежують поведінку користувача навіть після виходу із сайту, якщо не були застосовані засоби збереження приватності.

Кукі-зомбі – флешфайлів cookie, які автоматично відтворюються після того, як користувач їх видалив. Їх важко контролювати та неможливо видалити повністю. Використовуються в онлайн-іграх для запобігання шахрайству

користувачів, а також використовуються для встановлення шкідливого програмного забезпечення на пристрій користувача.

Тож за визначенням Офісу комісара з інформації Великобританії, не всі файли кукі виступають ідентифікаторами та обробляють персональні дані, а саме ті, які використовується для ідентифікації користувача при вході до облікового запису[567]. Кукі-файлів, які не обробляють персональні дані, служать для автоматичного налаштування мови сайту, не дозволяють зробити будь-які висновки про фізичну особу, з тим не підпадають під дію законодавства про захист персональних даних. У користувацьких угодах може передбачатись окреме застереження, що сайт або мережа не персоналізує дані, тобто не прив'язує їх конкретного користувача. У такий спосіб, інформуючи користувачів про прийняття належних мір безпеки та захисту персональних даних.

Як було зазначено вище, кукі-файли можуть використовуватися рекламодавцями для донесення певної інформації про товари та послуги до цільової аудиторії. Слід зазначити, що Регламент ЄС 2016/679 вимагає, щоб користувача було повідомлено про збір даних файлами cookie. Законодавство вимагає не лише отримання згоди користувача на використання цього стороннього cookie-файлу, а й надання користувачеві права відмовитися від використання такого cookie (opt-out) і можливості продовжувати відвідувати вебсайт незважаючи на відмову [312].

Тож кукі-файли необхідно розділяти залежно від можливості ідентифікувати суб'єкта: такі, що не дозволяють ідентифікувати користувача та такі, що дозоляють ідентифікувати. Використання останніх, потребує дотримання вимог законодавства про захист персональних даних щодо належного повідомлення та отримання належної згоди суб'єкта на обробку.

Серед таких ідентифікаторів слід назвати: ім'я, прізвище, дата і місце народження, статева приналежність, громадянства, індивідуальні страхові та податкові номери. Зазначені ідентифікатори відносяться до традиційних, використовуються в більшості держав світу, водночас можуть повторюватися, не можуть гарантувати повну ідентифікацію фізичної особи.

Окрім застосування традиційних засобів ідентифікації фізичних осіб із застосування цифрового коду та іншого нелітерального шифру, наразі активно як засоби ідентифікації використовуються біометричні дані. Майже до осені 2001 року використання систем біометричної ідентифікації було виключним правом воєнно-оборонного сектору та в меншій мірі комерційному секторі. Теракти 11 вересня 2001 року в США стали поштовхом для розвитку системи біометричної ідентифікації спершу у США, а потім і в усьому світі. У межах Міжнародної організації стандартизації (ISO) було створено підкомітет JTC 1/Sc37 з питань біометрії, метою якого є розробка єдиних стандартів використання біометричних даних [574].

Наразі поширення застосування систем біометричної ідентифікації обґрунтовано безпечністю та зручністю технології, розвитком цифрової ідентичності та платформі блокчейн, та цифровізацією державного управління [333].

Відповідно до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»[155] від 20 листопада 2012 р. № 5492-VI біометричними даними є сукупність даних про особу, зібраними на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри – відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук).

Стосовно застування біометричних даних в Україні С. Бригинець зазначає, що донедавна продовжувалася боротьба з «міткою звіра» [12]. Остаточну крапку в цьому питанні поставила постанова Верховного суду у складі колегії суддів Касаційного адміністративного суду 26.03.2018 р. у справі №806/3265/17 [135].

Відповідно до п. 14 ст. 4 Регламенту ЄС 2016/679 біометричні дані є персональними даними, які отримання внаслідок спеціальної технічної обробки, які стосуються фізичних, фізіологічних або поведінкових рис фізичної особи, а

також дозволяють або підтверджують ідентифікацію цієї фізичної особи, як наприклад, зображення особи або дактилоскопічні дані.

Як зазначається в Керівництві 3/2019 Європейського Правління з захисту персональних даних з обробки персональних даних із застосуванням відеопристроїв, щоб дані вважалися біометричні даними в розумінні Регламенту ЄС 2016/679, вони мають бути результатом спеціальної технічної обробки, різних вимірів фізичних, фізіологічних або поведінкових характеристик[714]. Відтак світлина, відео із фізичною особою як такі, не можуть вважатися біометричними даними відповідно до ст. 9 Регламенту ЄС 2016/679 лише за умови застосування спеціальної технічної обробки цих даних з метою сприяння однозначної ідентифікації фізичної особи. Для того, щоб це вважалося обробкою спеціальних категорій персональних даних (ст. 9), необхідно, щоб біометричні дані оброблялися з метою однозначної ідентифікації фізичної особи. Із аналізу п. 14 ст. 4 та ст. 9 Регламенту ЄС 2016/679 випливає, що необхідно враховувати такі критерії для того, щоб встановити, що обробляються біометричні персональні дані: характер даних, що вони стосуються фізичних, фізіологічних або поведінкових характеристик фізичної особи; засоби та способи обробки, вони мають бути «отримані в результаті конкретної технічної обробки»; мета обробки – дані повинні використовуватися з метою однозначної ідентифікації фізичної особи. За загальними правилом згідно зі ст. 9 Регламенту ЄС 2016/679, обробка біометричних даних з метою однозначної ідентифікації фізичної особи забороняється.

Крім того, такі ризики проявляються в тому, що біометричні дані переважно залишаються незмінними, або їх не можливо змінити способом, який був би пропорційний у порівнянні із ризикам. Ця обставина прямо або опосередковано простежується у визначенні біометричних персональних даних у передбачених документом «Про концепцію персональних даних», розробленим Робочою групою із захисту персональних даних ЄС [708]. За даним документом, біометричні дані мають розумітися як біологічні властивості фізіологічних характеристик, рис характеру, поведінки, яка є унікальною для

конкретного суб'єкта та яку можна емпірично спостерігати, навіть якщо вимірювання показників може нести характер вірогідності. Як приклад, відбитки пальців, сітківка ока, структура обличчя, геометрія рук, малюнок вени та поведінкові характеристики (підпис, манера натискання клавіш, хода та голос тощо). Також слід наголосити на дуалізмі біометричних персональних даних, які, з одного боку, надають інформацію про конкретну особу, а з іншого, характеристику існуючого зв'язку між відповідною інформацією та конкретну особу.

Закон Великобританії Про захист персональних даних 2018 року у розділі 205 містить визначення біометричних даних як персональних даних, які отримані в результаті спеціальної технічної обробки, що стосуються фізичних, фізіологічних або поведінкових характеристик особи, які дозволяють або підтверджують унікальну ідентифікацію цієї особи, наприклад, зображення обличчя або дактилоскопічні дані[452]. Унікальна ідентифікація осіб на основі біометричних даних є досить істотною, саме вона дозволяє відмежувати біометричні дані від інших видів даних. Використання біометричних даних дозволяє державним органам з високою точністю визначати місце перебування особи та її діяльність.

Аналіз розуміння функціонування технології біометричного автоматичного розпізнавання осіб за обличчям детально надано у справі Edward Bridge v. The Chief Constable of South Wales Police [404]. За визначенням Апеляційного суду, технологія автоматичного розпізнавання обличчя дозволяє перевірити, чи належать два різних зображення одній особі на основі біометричних даних (тобто вимірів або векторів рис обличчя), взятих із цифрової фотографії обличчя і порівняних з біометричними даними обличчя із зображень, що зберігаються в базі даних. Суд пояснив, що така технологія дозволяє отримати зображення обличчя будь-якої особи, що проходить повз камер відеоспостереження, встановлених у транспортних засобах правоохоронних органів або на дорогах загального користування. Аналогічним чином Суд зазначив, що такі камери дозволяють отримувати цифрові зображення обличчя

громадян, які фіксуються і обробляються в режимі реального часу для вилучення біометричної інформації про обличчя, яка порівнюється з біометричною інформацією, що міститься у «списку спостереження», підготовленому правоохоронними органами. Суд уточнив, що на основі зображень зі списків спостереження створюється «біометричний шаблон», який використовується для алгоритмічного порівняння з біометричними даними, отриманими з облич громадян, які перебувають на вулиці, беруть участь у публічних заходах. Суд зазначив, що якщо програмне забезпечення виявляє можливий збіг між зображеннями, зафіксованими камерами відеоспостереження, і зображенням зі списку розшукуваних осіб, працівники уповноважених органів будуть повідомлені про це для вжиття необхідних заходів (наприклад, арешту або допиту особи).

Ця справа також примітна тим, що детально описує процес автоматичного розпізнавання обличчя, який включає такі етапи (п. 9 Рішення Апеляційного суд): 1) складання (використання) існуючої бази даних зображень (для використання зображень з метою автоматичного розпізнавання обличчя, вони обробляються таким чином, щоб «риси обличчя», пов’язані з суб’єктами, були виражені у вигляді числових значень); 2) отримання зображення обличчя (камера відеоспостереження робить цифрові знімки зображень облич у режимі реального часу); 3) виявлення облич (після того, як камера відеоспостереження, яка використовується в режимі реального часу, знімає кадри, програмне забезпечення виявляє обличчя, а потім виокремлює конкретні обличчя); 4) вилучення ознак (в результаті вилучення обличчя, програмне забезпечення автоматично виокремлює унікальні риси обличчя із зображення кожного обличчя, в результаті чого біометричний шаблон стає унікальним для даного зображення); 5) порівняння обличчя (програмне забезпечення порівнює вилучені риси обличчя з тими, які містяться в зображеннях облич, що зберігаються в базі зображень); 6) встановлення співпадіння (під час порівняння рис обличчя на двох зображеннях програма розпізнавання визначає ступінь співпадіння). Ступінь співпадіння виражається в числовому значенні, вказує на ймовірність

співпадіння обличчя, де високе число вказує на високу ймовірність збігу двох облич. Якщо ступінь співпадіння вище встановленої межі, дані передаються для подальшої обробки фізичній особі для підтвердження (або спростування) співпадіння та вжиття заходів перевірки особи співробітниками правоохоронних органів. Якщо співпадіння не виявлено, відео, які надійшли з камери спостереження, автоматично видаляються.

З огляду на триваючу роботу над Проєктом Закону «Про єдину систему відеомоніторингу стану публічної безпеки» № 11031 який має запровадити правові засади застосування дистанційної біометричної ідентифікації фізичних осіб, необхідно у майбутньому Законі взяти за основу вищезазначену покрокову процедуру дистанційної ідентифікації. Передбачення такої норми в Законі покликано забезпечити прозорість застосування, етапи створення, розміщення баз даних та застування технології дистанційної біометричної ідентифікації.

Розрізняють динамічні та статистичні технології біометричної ідентифікації. Динамічні засновуються на поведінкових властивостях особи: ідентифікація за набиранням тексу на клавіатурі та написанням тексту; за голосом. Статистична ідентифікації ґрунтується на специфічних фізіологічних характеристиках, які особа має від народження, як наприклад: розпізнавання людини за райдужною оболонкою ока та сітківкою, термограмою і формою ока, відбитком пальців, розташуванням вен на долоні та її формою, ДНК[8, с. 137]. Поширення набуває використання ідентифікації за відбитком пальців, тривимірним зображенням обличчя та за райдужною оболонкою ока. Біометрична ідентифікація передбачає отримання відбитку за допомогою спеціального сканера, який перетворює зображення на цифровий код і порівнюється з раніше введеним еталоном також із застосуванням сканеру для зчитування.

Відносно поширеною залишається ідентифікація осіб за відбитками пальців, яка заснована на унікальності малюнка папілярних візерунків на пальцях. Перші відомості про ідентифікацію особистості за папілярними лініями

датовані 300 роком до н.е. (Китай) і 702 роком до н.е. (Японія), проте така ідентифікація не була біометричною.

Наступним є ідентифікація за сітківкою ока, заснована на унікальності малюнка судин дна ока. У процесі сканування, всередину ока спрямовується промінь червоного світла, а обличчя розташовується навпроти сканера. Така система ідентифікації має низький відсоток помилкової ідентифікації. Недоліком є – негативний вплив у разі захворювання ока (катаракті або глаукомі). Ідентифікація за малюнком райдужної оболонки ока, що має високу унікальність, передбачає, що сканування відбувається шляхом фотографування обличчя (камерою з високою роздільною здатністю) і виділення на ньому райдужної оболонки, зображення якої вимірюється із застосуванням технічної обробки, створюючи цифровий шаблон. Оскільки можлива поява пігментних плям або зміна кольору райдужної оболонки, використовують чорно-біле зображення. На точність результату ідентифікації можуть впливати навіть незначні травми ока або безсоння, що є недоліком [315, с. 59].

Ідентифікація за характеристиками долоні передбачає створення тривимірного відбитка кисті руки (геометрія кисті, об’єм пальців, нерівності долоні, розміщення складок шкіри) або зняття термограми розташування судин на зовнішній стороні долоні. Цей малюнок є неповторним і стабільним протягом усього життя людини, порізи або забруднення не є перешкодою для порівняння.

У процесі біометричної ідентифікації за формою обличчя створюється тривимірний образ обличчя із використанням відеокамери (високої роздільної здатності), визначаються контури брів, очей, носа, губ, підборіддя, вух, відстань між ними, а також прогнозується низка варіантів зміни образу залежно від повороту обличчя, нахилу, зміни міміки тощо. Цифровий образ обличчя зберігається в базі та служить для порівняння зображення обличчя. Недоліком є неточність ідентифікації у випадку використання аксесуарів: окуляри, накладні вуса, борода, грим тощо.

Біометрична ідентифікація за термограмою обличчя засновується на унікальності розміщення артерій на обличчі, які живлять кров’ю шкіру та

виділяють тепло. Для отримання термограми застосовуються спеціальні камери інфрачервоного світла, які функціонують навіть у темну добу, результат розпізнавання не залежить від різких перепадів температури обличчя, старіння шкіри, оперативного втручання, гриму, штучних елементів тощо. Такий метод надає можливість відрізнити близнюків, є ефективнішим ніж 2D- або 3D-сканування.

Метод ідентифікація за голосом базується на теорії, що кожен голос є унікальним. Технологія, як правило, спирається на цифрове відображення звукових хвиль, що виникають, коли особа вимовляє певні слова або низку слів; коли особа намагається отримати доступ до системи після реєстрації, необхідно вимовити слова для їх розпізнавання та порівняння із збереженими у системі. Верифікація голосу може бути не такою точною як інші біометричні методи, такі як сканування пальців та розпізнавання райдужної оболонки ока, але вона може бути єдиною технологією, доступною в певних сферах використання (наприклад, при здійсненні телефонних транзакцій) [315, с. 59].

Окремо слід зазначити, про «поведінкову» біометрію або динамічні методи біометричної автентифікації, які засновуються не на рисах зовнішності, а на індивідуальних особливостях вчинення дій особою. Оскільки кожна людина унікально ставить підпис та набирає текст на клавіатурі, динамічні методи біометричної автентифікації дозволяють аналізувати напрямок, швидкість, натискання клавіатури та підписання документів, порівнюючи із попередніми зразками [315, с. 59]. Слід зазначити, що електронні панелі для підпису, які використовуються майданчиками електронної комерції та поштовими сервісами для укладення договорів купівлі-продажу, замовлення товарів та послуг, переважно не застосовують біометричні методи автентифікації, а створюють файл цифрового зображення підпису для подальшого його використання. Існує твердження, що динамічні методи біометричної автентифікації не є біометрією в «чистому вигляді», адже не дозволяють із таким же рівнем точності як статистичні методи біометрії, ідентифікувати суб’єкта даних [693, с. 5]. З

урахуванням рівня розвитку технологій, з даним твердженням складно погодитися.

Окремі методи ідентифікації, такі як біометрична ідентифікація за відбитками пальців, сітківки ока та райдужної оболонки ока, отримали переважне застосування в той час, як решта втратила свою частку ринку. Наразі Агентство перспективних оборонних дослідницьких проєктів США веде розробку нового типу біометричної віддаленої ідентифікації особи, яка включає визначення характерної ходи людини [693, с. 5].

Управління Верховного комісара ООН у справах біженців, використовує біометричні сканування райдужної оболонки ока для посвідчення особи біженця, перевірки балансу, рахунку, підтвердження покупок, вчинення покупок у супермаркетах біженцями тощо. Всесвітня продовольча програма ООН використовує біометричну ідентифікацію у проєкті «Блокчейн проти голоду» [875].

Таким чином біометричні дані мають визнаватися як персональні дані, що отримані внаслідок спеціальної технічної обробки, що стосуються фізичних, фізіологічних або поведінкових характеристик особи, які дозволяють однозначно ідентифікувати цю особу. Біометрична ідентифікація може проводитися за такими ідентифікаторами: зображення обличчя, відбитки пальців, сітківки ока, райдужна оболонки ока, формою обличчя, термограмою обличчя, геометрія рук, малюнок вени та поведінкові характеристики (підпис, манера натискання клавіш, хода або манера мовлення тощо).

Окремо слід приділити увагу такій категорії даних як спеціальні категорії персональних даних, які розкривають расову або етнічну приналежність, політичні погляди, релігійні переконання або філософські погляди, членство у профспілкових організаціях (п. 71, 75, Преамбули Регламенту ЄС 2016/679). До даних, пов’язаних з расовим або етнічним походженням відносяться: ім’я, місце народження, рідна мова, імена батьків, оскільки можуть свідчити про походження людини або її етнічну приналежність, тому відносяться до чутливих даних. Політичні переконання можна вивести, виходячи з аналізу діяльності, що

розкриває політичні вподобання людини, до яких відносяться членство в політичній партії, підписані петиції, мітинги або протести, в яких особа брала участь. Інформація, що відображає ідеї, які вона підтримує або навпаки, можуть розкривати політичні погляди індивіда.

Такі дані як відвідування релігійної організації, придбання релігійних книг, участь у релігійних заходах або демонстраціях свідчить про те, що особа сповідує певну релігію або проявляє інтерес, допомагають розкрити релігійну приналежність або свідчити про відсутність у особи релігійних переконань. У британському прецеденті Grainger Plc v. Nicholson [385] термін «філософські переконання» охоплює таку категорію як «релігійні переконання». Відповідач відносить до філософських переконань широке коло переконань, які стосуються важливих аспектів життя та поведінки, та які вимагають поваги в демократичному суспільстві. Відтак до спеціальної категорії даних відноситься інформація про членство у профспілковій організації. Оскільки такі дані потенційно можуть призводити до дискримінації на робочому місці, що може бути потенційним наслідком її профспілкової діяльності та впливати на ведення колективних переговорів.

За ст. 4 Регламенту ЄС 2016/679 до фізичних та психологічних даних відноситься інформація, яка стосується відвідувань лікаря або фахівців у сфері охорони здоров’я, отримання медичних послуг, діагностування перенесених захворювань або інші факти про стан здоров’я, як-то серцевий ритм, пульс, артеріальний тиск, інші результати медичних аналізів, які інформують про стан здоров’я та потребують відповідного захисту. Через те, що дані про особу можуть бути розкриті опосередковано через її партнера, то такі дані будучи чутливими, потребують додаткового захисту. Дані особистого життя, можуть випливати з інших даних, таких як читана література, документи, історія відвідування сайтів, даних із сайтів знайомств, участь у організаціях, заходах та демонстраціях.

Як зазначає Р.Б. Шишка, з поширенням інформаційно-комунікаційних технологій постає потреба в розробці та застосуванні універсального

ідентифікатора особи, за яким фізична особа підлягає ідентифікації в публічних та приватних відносинах під час проведення безготівкових розрахунків, соціальних виплат тощо. Науковець пов'язує використання таких ідентифікаторів із технологіями трансплантації електронних пристроїв у тіло людини, так званих homo virtualis [277, с. 16] або Homo Supertechnologics.

Розмірковування з приводу надійних засобів ідентифікації особи приводить науковців до висновків про те, що постійність та унікальність такої ознаки повинна мати у своїй основі складові біометричних персональних даних, а саме геномну інформацію (дані ДНК). У науці висувається думка, що запровадження обов'язкової геномної реєстрації при народженні дозволило б створити базу даних ДНК, де відповідному біологічному матеріалу особи було б присвоєно цифровий номер або буквено-цифровий код. Такий номер, будучи незмінним протягом життя, мав би використовуватися в актових записах та документах, які засвідчують особу, поряд з ім'ям. У такому випадку зміну імені можна було б нівелювати індивідуальним номером (кодом) геномної інформації. Слід зазначити, що реалізація даної пропозиції є вельми дискусійною темою.

Відповідно до п. 34 Преамбули та ст. 4 (13) Регламенту ЄС 2016/679, під генетичними даними розуміють персональні дані щодо спадкових або набутих генетичних характеристик, які отримані в результаті аналізу біологічного зразка фізичної особи, зокрема аналіз хромосом, дезоксирибонуклеїнової кислоти (ДНК) або рибонуклеїнової кислоти (РНК), або в результаті аналізу інших елементів, що дозволяють отримати еквівалентну інформацію. Збір, обробка будь-яких чутливих даних, у тому числі генетичних даних за загальним правилом забороняється, за винятком спеціально передбаченим законодавством.

Геномна реєстрація заснована на проведенні молекулярно-генетичної експертизи людини, яка покликана забезпечити правовий механізм ідентифікації фізичної особи із точністю та незмінністю провідного ідентифікатора. Результати молекулярно-генетичної експертизи є надійним доказом, який ефективно використовується для встановлення сімейних відносин та є єдиним

науковим методом, який дозоляє точно встановити батьківство особи, про що зазначає ЄСПЛ у своїх рішеннях.

Із ратифікацією Законом України від 20.06.2012 [164] Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства, Україною взято на себе низку зобов'язань, зокрема щодо збору та накопичення ідентифікаційних даних та ДНК осіб, засуджених за вчинення правопорушень, передбачених Конвенцією. Наразі з огляду на потребу проведення Експертною службою МВС молекулярно-генетичних досліджень, пов'язаних із вчиненням воєнних злочинів на території України, Верховна Рада України прийняла важливий для правоохоронної системи та сфери експертно-криміналістичної діяльності закон – «Про державну реєстрацію геномної інформації людини» № 4265 [148]. Закон урегульовує процеси створення і функціонування обліку геномної інформації людини, покликаний удосконалити роботу правоохоронних органів із розслідування злочинів та встановлення осіб, які їх вчинили, ефективніше проводити розшук зниклих безвісти та ідентифікації невпізнаних осіб. Прийнятий закон передбачає створення єдиної державної бази даних ДНК доступ до якої з метою перевірки має бути наданий колу правоохоронних органів та органів розвідувальної діяльності у встановленому порядку. Передбачається добровільне та обов'язкове проведення державної реєстрація геномної інформації.

Світовий досвід ведення подібних реєстрів свідчить про практику створення єдиної бази даних ДНК, із одним держателем та адміністратором бази даних [126]. У США та Великобританії ведуться бази даних, до яких вносяться профілі ДНК осіб, засуджених за вчинення злочини [530].

Відповідно до п. 6 ч. 1 ст.1 Закону України «Про державну реєстрацію геномної інформації», молекулярно-генетичною експертизою (дослідженням) визначається – дослідження біологічного матеріалу людини, що здійснюється з метою отримання її геномної інформації. Ст. 5 Закону України «Про державну реєстрацію геномної інформації» передбачає категорію осіб щодо яких має

провадитися обов'язкова державна реєстрація геномної інформації, за рахунок коштів державного бюджету, а саме:

1) осіб, притягнутих до кримінальної відповідальності у вчиненні умисних тяжких чи особливо тяжких злочинів проти основ національної безпеки України, життя, здоров'я, волі, честі, гідності, статевої свободи та статевої недоторканості особи, власності, громадської безпеки, у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, проти миру, безпеки людства та міжнародного правопорядку, або щодо яких обрано запобіжний захід;

2) осіб, які вчинили суспільно небезпечні діяння або злочини проти основ національної безпеки України, життя, здоров'я, волі, честі, гідності, статевої свободи та статевої недоторканості особи, власності, громадської безпеки, у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, проти миру, безпеки людства та міжнародного правопорядку, та до яких за рішенням суду застосовані примусові заходи медичного характеру;

3) осіб, засуджених за вчинення умисних злочинів проти основ національної безпеки України, життя, здоров'я, волі, честі, гідності, статевої свободи та статевої недоторканності особи, власності, громадської безпеки, у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, проти миру, безпеки людства та міжнародного правопорядку;

4) установлена з біологічного матеріалу, отриманого під час проведення слідчих (розшукових) дій з місця вчинення кримінального правопорушення, скоєного в умовах неочевидності, або отримано під час досудового розслідування та неідентифіковано;

5) невпізнаних трупів людей, їх останків та частин тіла людини, відомості про виявлення яких внесено до Єдиного реєстру досудових розслідувань або розпочато розслідування;

6) встановлена з раніше відібраних біологічних зразків осіб, зниклих безвісти, або біологічного матеріалу з особистих речей осіб, зниклих безвісти, відомості щодо яких внесено до Єдиного реєстру досудових розслідувань або розпочато розслідування;

7) осіб, які не здатні через стан здоров'я, вік або інші обставини повідомити інформацію про себе.

Крім того, ст. 8 Закону передбачає відбір біологічного матеріалу у військовослужбовців, поліцейських, осіб рядового та начальницького складу служби цивільного захисту, добровольчих формувань територіальних громад за їх заявою, у випадку введення воєнного стану в обов'язковому порядку. Порядок та строки відбору, строки зберігання біологічного матеріалу щодо даних категорій осіб має визначатися Міністерством оборони України, Міністерством внутрішніх справ України, Службою безпеки України, Управлінням державної охорони України, розвідувальним органом, Державною службою спеціального зв'язку та захисту інформації України, Кабінетом Міністрів України.

Наразі практика українських судів свідчить, що передбачене проведення обов'язкової молекуляро-генетичної експертизи для окремих категорій осіб, зокрема військовослужбовців, стає провідним належним доказом для встановлення фактів, що мають юридичне значення [177; 178; 179; 180; 181; 182; 183].

Поряд із обов'язковою державною реєстрацією Законом передбачена добровільна державна реєстрація геномної інформації, яка проводиться за рахунок власних коштів особи, на підставі письмової заяви особи про відбір у неї біологічного матеріалу, проведення молекулярно-генетичного дослідження та внесення інформації до Електронного реєстру.

Вказані законодавчі новели піддаються критиці науковцями. О.М. Калітенко ставить під сумнів передання реєстрації найціннішої інформації про людину, її генетичного коду на платній основі – порядок та вартість якої має додатково встановлюватися Кабінетом Міністрів України. Залишається неврегульованою процедура та порядок знищення геномної інформації після сплину строку її зберігання. Давши загальне визначення біологічного матеріалу, під яким розуміється тканина та виділення тіла людини, останків померлої людини, що містять геномну інформацію людини, законодавець не передбачив конкретний перелік об'єктів біологічного походження, які мають бути відібрані

для проведення молекулярно-генетичної експертизи. У фахівця, який відбирає такий матеріал, можуть виникнути труднощі з реалізацією окремих положень закону (наприклад, здійснення відбору біологічних зразків уповноваженою особою органу (установи) виконання покарань або органу з питань пробації[72, с. 607].

Законом передбачено створення Електронного реєстру геномної інформації людини – інформаційно-комунікаційна система, що забезпечує збирання, реєстрацію, накопичення, зберігання, поновлення, пошук, використання і поширення (розповсюдження, передачу) геномної інформації людини.

Результати молекулярно-генетичної експертизи є найнадійнішим доказом встановлення сімейних зв'язків та є єдиним науковим методом, який дозоляє точно встановити батьківство особи, про що зазначає ЄСПЛ. Слід зазначити, що в кожної з клітин людини є 23 пари хромосом, частину з яких людина отримує від матері, а іншу частину від батька. Такими чином кожна людина, яка проходить молекулярно-генетичну експертизу, «відображає» не лише дані про власну особу, але й сотні інших людей, які знаходяться з нею в родинних відносинах. Наприклад, саме завдяки співробітництву незалежної генеалогічної платформи GEDmatch, які збирають ДНК для пошуку родичів зі всього світу, та правоохоронних органів США через багато років після вчинення злочинку вдалося встановити та притягнути до відповідальності ґвалтівника Джозефа Джеймса Діанджело [280].

Враховуючи викладене, з огляду на чутливість даних, що збираються для проведення молекулярно-генетичної експертизи, існує високий ризик втручання у приватне життя людини, ЄСПЛ у своїх рішеннях неодноразово наголошував, що використання технологій збору та обробки даних може ставити під загрозу втручання та зловживання правами людини. Конвенція Ради Європи про захист осіб при автоматизованій обробці персональних даних від 28 січня 1981 року № 108 [819] та Директива ЄС 95/46/ЄС «Про захист фізичних осіб під час обробки персональних даних та про вільне переміщення таких даних» від 24 жовтня 1995

року передбачають захист права на особисте життя у зв’язку з обробкою персональних даних. Рекомендація Комітету Міністрів Ради Європи № R(92)1 від 9 квітня 1992 року[721] встановлює, що зразки, які були взяті для аналізу ДНК, не повинні зберігатися після винесення остаточного рішення у справі, в якій їх було використано, окрім випадків, коли це необхідно для цілей, безпосередньо пов’язаних із цілями їх збору, а також у разі, якщо особу, якій вони належать, суд визнав винною у скоєнні тяжких злочинів проти життя, недоторканності та безпеки інших осіб.

Як наголошує ЄСПЛ, збір та обробка державними органами даних про фізичних осіб вимагає дотримання справедливого балансу приватних та публічних інтересів. У справі S. and Marper vs the United Kingdom 2008 року [408], щодо безстрокового зберігання в базі даних відбитків пальців, зразків клітин та профілів ДНК заявників, після того, як кримінальне провадження по відношенню до одного із підозрюваних припинено, а другого – виправдано, ЄСПЛ зазначив, що використання сучасних наукових методів у кримінальному судочинстві будь-якою цінною є неприпустимим. Потребує дотримання балансу між потенційною вигодою від використання подібних методів та інтересами, зумовленими невтручанням у приватне життя. Суд дійшов висновку, що беззастережний та невибірковий характер повноважень, пов’язаних із зберіганням відбитків пальців, зразків клітин та профілів ДНК осіб, які підозрювалися у скоєнні злочинів та не були засуджені за них, як це мало місце в даному випадку, не забезпечує дотримання справедливого балансу між публічними та приватними інтересами.

Серед засобів забезпечення ідентифікації користувачів окремих мережевих ресурсів називають інструменти електронного підпису[23]. Участь у цивільному обігу, належне укладення правочинів у мережі потребує їх підписання сторонами. Частина 3 ст. 207 ЦК України передбачає можливість використання у разі вчинення правочинів факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, електронно-числового підпису або іншого аналога власноручного підпису у випадках, встановлених

законом, іншими актами цивільного законодавства, або за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів.

З метою гармонізації українського законодавства із законодавством Європейського Союзу, зокрема Директива 1999/93/ЄС Європейського Парламенту та Ради від 13.12.1999 «Про систему електронних підписів, що застосовується в межах Співтовариства» [165], імплементацію законодавства ЄС у сфері електронної ідентифікації було прийнято Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 5.11.2017 № 2155-VIII [152], який закладає засади ідентифікації суб'єктів в інформаційних відносинах під час надання держаних послуг. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» запровадив поняття кваліфікованого електронного підпису (далі КЕП) замість електронного цифрового підпису, який визначається як удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа (п. 23 ст. 1 Закону). КЕП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Система цифрового підпису припускає, що кожен користувач мережі має свій особистий ключ (що зберігається в таємниці), який використовується для формування підпису, а також відповідний цьому особистому ключу відкритий ключ, відомий решті користувачів мережі і призначений для перевірки підпису. Цифровий підпис обчислюється на основі особистого ключа відправника інформації й власне інформаційних бітів документа (файлу). Спосіб обчислення цифрового підпису гарантує, що знання відкритого ключа не може призвести до підробки підпису. Токен – компактний пристрій, призначений для забезпечення інформаційної безпеки, ідентифікації власника, безпечного віддаленого доступу до інформаційних ресурсів.

Відповідно до ст. 18 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» кваліфікований електронний підпис за юридичною силою прирівняний до власноручного підпису.

КЕП накладений на документ виконує такі функції: ідентифікації автора підпису (ПІБ, фізична чи юридична особа, ІНН чи ЄДРПОУ); підтвердження факту внесення змін у документ після його підписання; захист документа від фальсифікації та підроблення; фіксація часу, що дозволяє підтвердити достовірність проставлення підпису, навіть після сплину строку чинності сертифіката, анулювання або відкликання [112].

Використання КЕП отримало поширення у професійній діяльності державних службовців, співробітників правоохоронних органів, діяльності державних реєстраторів відповідно до положень Законів України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» та «Про державну реєстрацію юридичних осіб, фізичних осіб підприємців та громадських формувань» та інших сферах[149; 150].

Подекуди як синоніми використовують такі категорії як «цифровий підпис» та «електронний підпис», водночас вони виконують різні функції, хоча й служать для встановлення автентичності цілісності документів, хоча й різними способами [51, с. 213]. Серед відмінностей електронного та цифрового підпису слід назвати наступне. Електронний підпис містить менше засобів безпеки ніж цифровий, його збереження забезпечуються криптографічними методами шифрування, які не підлягають підробленню, забезпечують можливість відстеження, дозволяють сторонам встановити чи вносилися в документ зміни, їх час та особу, яка поставила підпис. Електронні підписи, є також досить захищеними, проте, не відповідають таким же суворим вимогам як цифрові підписи. Цифровий підпис підлягає перевірці, завдяки стандартам шифрування. Відрізняється мета використання цифрового підпису та електронного підпису, якщо метою цифрового підпису є захист документа, переконання в його справжності та незмінності. Якщо цифровий підпис використовується для підтвердження автентичності документа, то електронний підпис засвідчує згоду особи з умовами договору. Зазвичай обидва види підписів можуть бути використані одночасно, для посвідчення правочину або досягнення домовленості сторонами за договором.

З метою ідентифікації особи для оформлення, видачі, обміну, пересилання, вилучення, повернення державі, визнання недійсними документів, визначених Законом, а також у межах, визначених законодавством про свободу пересування та вільний вибір місця проживання, ведення обліку інформації про реєстрацію місця проживання чи місця перебування особи ведеться Єдиний державний демографічний реєстр відповідно до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»[155] та Порядку ведення Єдиного державного демографічного реєстру та надання з нього інформації, взаємодії між уповноваженими суб'єктами, а також здійснення ідентифікації та верифікації затвердженого постановою Кабінету Міністрів України від 18 жовтня 2017 р. № 784 [134].

Законодавець передбачив об'єднання більшості юридично значущих даних кожної фізичної особи в індивідуальний запис реєстру, позначений за допомогою унікального номера. Тобто в єдиний реєстр, який ведеться Державною міграційною службою як розпорядником Єдиного державного демографічного реєстру зібрана інформація, що ідентифікує особу, яка міститься в інформаційних базах даних різних державних органів та відомств. Саме по собі переміщення розрізненої інформації, в єдине «досьє», не змінить ані якості, ані властивостей наявних нині в розпорядженні держави додаткових ідентифікаторів фізичних осіб, а лише полегшить збирання, пошук та використання даних. Оперативність і якість процесів формування реєстру, доступу до його даних, зберігання й опрацювання цих даних, а також інші процедурні питання функціонування реєстру поки що не дістали нормативно оформленого вирішення. Тому видається, що ідея створення такого реєстру зі всією масштабністю даних, які збираються, не вирішує повною мірою питання ідентифікації суб'єкта правовідносин.

Стосовно паспорта можна зазначити, що паспорт у вигляді картки або книжечки традиційно досі використовувався для посвідчення фізичної особи. Хоча функції ідентифікації під час надання документа, який посвідчує особу

особисто, наразі прагне повторити ідентифікацію та автентифікацію в мережі, слід констатувати певні відмінності. По-перше, документи, що посвідчують особу, такі як паспорт, пред'являються особисто, а людина, будучи присутньою, займає провідне місце у процесі ідентифікації. По-друге, хоча вочевидь, що документи, що посвідчують особу, необхідні для ухвалення рішення уповноваженою посадовою особою (працівником прикордонної служби), подібне рішення вимагає судження, заснованого зокрема, на безпосередньому спостереженні за особою, яка підлягає ідентифікації. Будь-яке рішення, ухвалене працівником, ґрунтується на його судженні та власному розсуді, подекуди суб'єктивному.

На відміну від паспорта, який посвідчує особу, вирішальну роль під час ідентифікації та автентифікації в мережі відіграють дані, які є ідентифікаторами особи, а не людина, яку ідентифікують, коли вона пред'являє посвідчення особи або надала дані у разі віддаленої ідентифікації. Інформаційна система шукає відповідність між пред'явленою інформацією та даними, що містяться в системі. Важливо, що ідентифікація особи в мережі – це не просто ідентифікація людини. Незалежно від того, пред'являється ідентифікаційна інформація особисто чи віддалено, якщо вся інформація, пред'явлена в момент вчинення правочину, збігається з інформацією, що міститься в системі, то система автоматично дозволяє проведення операції з цією особою. У межах цих параметрів система, на думку Д. Дерема, може діяти сама[475, с. 14], щоб розпізнати певний набір даних, що становлять ідентифікаційні дані для проведення правочину, а потім провести правочин із зареєстрованими ідентифікаційними даними.

Підсумовуючи викладене, слід констатувати, що питання віднесення тих чи інших даних до таких, що є ідентифікуючими та дозволяють встановити конкретного суб'єкта, може варіюватися в залежності від рівня розвитку технологій (state of art) та співвідношення даних. Встановлення, що дані відносно суб'єкта є ідентифікаторами або ідентифікуючими ознаками, носить практичний характер у діяльності офіцера із захисту персональних даних компанії. Визнання даних такими, що дозволяють конкретно ідентифікувати суб'єкта, вимагає від

компанії як процесора або контролера прийняття всього спектру заходів для забезпечення належного збору, обробки, зберігання цих даних, недопущення витоків, постійний моніторинг та впровадження новітніх технічних заходів безпеки, дотримання вимог суб'єктів про сповіщення в разі будь-яких порушень щодо цілісності даних [705] тощо.

Підсумовуючи викладене, можна констатувати, що відбувається технологічне удосконалення засобів ідентифікації та поступове розширення сфер її застосування, збільшення обсягів персональних даних які збираються та обробляються в мережі. Поряд із цим, зростають ризики, що персональні дані можуть ставати доступними третім особам в результаті витоків, що вимагає застосування необхідних механізмів технічного та організаційного характеру для забезпечення належного захисту та безпеки. Створення та розробка безпечних цифрових технологій має стати провідним чинником для забезпечення довіри користувачів до них. Досягнення належного рівня безпеки має сприяти ефективному здійсненню ідентифікації фізичних осіб в мережі та, відповідно, забезпеченню довіри користувачів до новітніх технологій.

3. ЦИВІЛЬНА ПРАВОЗДАТНІСТЬ ТА ДІЄЗДАТНІСТЬ ФІЗИЧНОЇ ОСОБИ У ВІДНОСИНАХ У МЕРЕЖІ «ІНТЕРНЕТ»: ЛЕГАЛЬНІ ПІДХОДИ І ДОКТРИНАЛЬНІ ТЛУМАЧЕННЯ

3.1. Виникнення і припинення правоздатності та дієздатності фізичної особи в мережі «Інтернет»

Відзначимо, що динаміка правосуб'єктності фізичної особи є не біологічним, а юридичним процесом. Наприклад, припинення правової суб'єктності фіксується рішенням суду про оголошення фізичної особи померлою, лікарським свідоцтвом про смерть, свідоцтвом про смерть тощо.

Як зазначає В.А. Січевлюк, дієздатність фізичної особи не є її постійним атрибутом, що обумовлюється природними обставинами природними причинами, тобто ця дієздатність має етапи формування, вона передбачає первинне становлення, а також може за життя фізичної особи бути втрачена та відновлена. Характерно, що у фізичних осіб інші елементи правосуб'єктності правоздатність і деліктоздатність, загалом зростають чи занепадають поетапно та пропорційно до стадій становлення чи втрати її власної дієздатності [192, с. 41].

Особливості здійснення прав та обов'язків у мережі полягають у тому, що не всі фізичні особи мають доступ до інтернету, необхідні навички та компетенції для користування нею, можливістю користуватися електронними сервісами та КЕП, тому для таких осіб доступ до державних адміністративних послуг, сервісів електронної комерції може виявитися обмеженим або загалом недоступним. Відсутність навичок та компетенцій користування сервісами в мережі, відмова від реєстрації на сервісах, де умовою надання послуг є наявність акаунту користувача, позбавляє особу ефективно власними діями здійснювати надані їй права та виконувати обв'язки.

Уявляється, доцільним для здійснення прав та обов'язків при користуванні сервісами в мережі «Інтернет» та здійснення правоздатності та дієздатності

використовувати такі терміни як: цифрова правосуб'єктність, цифрова правоздатність та цифрова дієздатність.

Р.Б. Шишка зазначає, що цифрова правоздатність, заснована на знаннях, вміннях та компетентності в цифрових технологіях, наявності відповідного гаджета чи доступу до нього, персоніфікації як учасника цих відносин, чіпування. Її можна визначити як здатність основану на цифрових речах та технологіях сприймати, використовувати, набувати нові права та нести обов'язки [269, с. 127]. Можна солідаризуватися з Р.Б. Шишкою, який визнає цифроздатність сучасним проявом дієздатності.

Здатність мати цивільні права та обов'язки (цивільну правоздатність) мають усі фізичні особи з моменту їх народження. Передбачена охорона інтересів зачатої але не народженої дитини (ч. 1 ст. 25 ЦК України). Цивільна правоздатність будучи абстрактною можливістю володіти цивільними правами та нести обов'язки, не свідчить про те, що особа має конкретні права та обов'язки. Адже суб'єктивні права виникають відповідно до змісту та з урахуванням правоздатності. Цифрову правосуб'єктність або правосуб'єктність фізичної особи в мережі «Інтернет» слід розуміти як здатність виступати суб'єктом правовідносин в мережі «Інтернет», яка включає цифрову правоздатність та дієздатність. За аналогією цифрову правоздатність слід розуміти як здатність мати права та нести обов'язки в мережі «Інтернет».

Попри існування різноманітних дискусій, з приводу моменту виникнення правоздатності, загальновизнаним у вітчизняній науці вважається положення про те, що правоздатність виникає із моменту народження[270, с. 127]. В умовах інформаційного суспільства знову постає питання встановлення набуття фізичною особою правоздатності, коли особа набуває цифрової правоздатності в інтернеті. Чи слід визнавати виникнення – з моменту реєстрації на сайті та створення акаунту, чи вході на сторінку (сайт), чи вході в мережу «Інтернет» тощо.

Якщо припустити можливість застосування правових норм за аналогією, проаналізувавши положення чинного законодавства, тоді цифрова

правоздатність визнається рівною мірою за всіма фізичними особами та виникає з моменту народження та припиняється смертю. І в даному випадку постають окремі питання.

Висувається твердження, що правоздатність у мережі «Інтернет» у фізичної особи існує незалежно від волі, визнання або невизнання державою, а користувачі фактично використовують всю цифрову інфраструктуру відповідно до власних цілей та інтересів. Фізична особа в цифровому середовищі набуває для себе права та обов'язки, коли стає користувачем мережі «Інтернет». Правоздатність у мережі «Інтернет» як потенційна можливість використання цифрових технологій виникає з моменту народження людини, проте опосередковується моментом формування в користувача інфраструктури та фактом набуття доступу до мережі «Інтернет». Поряд із підключенням до мережі, виникнення правоздатності в мережі пов'язують із створенням сторінки в соціальній мережі, цифрового аватара, кодування штучного інтелекту тощо [215, с. 57]. Вважаємо, що означений підхід виникнення правоздатності фізичної особи є властивим вільному інтернету, за яким у фізичної особи виникає цілий спектр прав (право на недоторканність приватного життя, право на цифрову ідентичність, право не бути суб'єктом автоматизованого прийняття рішення, право на видалення тощо) та персональні дані щодо неї починають оброблятися та збиратися вже з моменту здійснення права доступу до інтернету, без необхідності виконання формальностей щодо реєстрації акаунта (профайлу) на сайті цифрового сервісу.

Слід зазначити, що у зв'язку з розвитком прав людини під впливом цифрового середовища, обсяг прав та обов'язків, а з тим і зміст правоздатності істотним чином розширюється через появу та стрімкий розвиток нових особистих немайнових прав (цифрових прав), що характеризуються специфічними властивостями та власним змістом.

Існує позиція науковців, що правоздатність у мережі «Інтернет» як здатність кожної особи мати права та обов'язки в цифровому середовищі не залежить від громадянства, а приналежність до громадянства тієї чи іншої

держави в мережі втрачає вирішальне значення. Оскільки цифрове середовище охоплює всі процеси, засоби взаємодії, сайти та цифрову інфраструктуру, громадянство певної держави для цифрової правосуб'єктності не несе значущої ролі. В умовах транскордонного характеру правовідносин, традиційний інститут громадянства в інтернеті не відіграє істотної ролі для виникнення правоздатності, а через відкриті можливості інтернету створюються уявлення, що фізична особа перестає бути пов'язаною з територією та законодавством певної держави [215, с. 57]. Постає питання, чи дійсно така теза відповідає дійсності. До того ж транскордонний характер відносин у мережі обумовив розробку категорії цифрового громадянства.

Як нам уявляється, означену тезу слід приймати із застереженням, оскільки здійснення цифрових прав фізичними особами значною мірою залежить від підходу держав до правового регулювання відносин в інтернеті. Так, потрапити із західного в китайський інтернет, може бути ускладнено або навіть неможливо. Деякі китайські урядові сайти не відкриваються, блокуючи користувачів з певних географічних регіонів. Інші платформи вимагають авторизації на сайті із китайським номером телефону, який прив'язаний до офіційного посвідчення особи. Файли та сайти можуть стати недоступними з перебігом років [878].

Означена теза відображає лише один із підходів у правовому регулюванні відносин у мережі «Інтернет» та потребує уточнення, оскільки здійснення прав у мережі «Інтернет» може істотно варіюватися, залежно від держави та механізмів правового регулювання прав та обов'язків у мережі, будь-то вільний, ліберальній підхід, властивий західному підходу регулювання (ЄС, США) або авторитарний підхід, властивий закритому, східному підходу регулювання інтернету (КНР).

Слід відзначити своєрідний підхід до врегулювання суспільних відносин у КНР, який відрізняється від західних традицій[220, с. 202]. Так, у КНР проводиться суворий контроль за публікаціями, коментарями користувачів соціальних мереж як основним засобом комунікації в інтернеті, а сайти та цифрові сервіси вимагають проходження реєстрації відповідно до автентичних,

реальних ПІБ та адресою. Обов'язковій реєстрації підлягають усі користувачі як блогери, так і коментатори, які воліють залишити коментар.

З 2006 року в КНР спеціально правоохоронне відомство проводить моніторинг та контроль за публікаціями та користувачами в мережі. З 2015 по 2017 роки було видалено майже 10 млн акаунтів користувачів у соціальних мережах та відмовлено реєстрації за власними справжнім іменем. За твердженням уряду КНР, така політика дозволяє підвищити рівень науковості та культури серед коментарів, сприяє здоровому розвитку спільноти, захищає інтереси громадян, юридичних осіб, державну безпеку та суспільні інтереси в інтернеті [186].

Незалежно від місця знаходження фізичної особи, як-то на території КНР так і поза її межами, її акаунт, публікації в китайських додатках та цифрових сервісах підлягають перевірці та цензурі. Властивістю китайських додатків WeChat та Alipay, від аналогічних сервісів, створених для громадян КНР, які проживають у США, як ChineseInLA.com є те, що уряд КНР має постійний доступ до них та можливість проведення перевірок користувачів. Так, поширеною практикою є зникнення публікації чутливого контенту впродовж 10 хвилин, що неминуче приводить до постійного самоцензурування користувачами [83; 305; 624]. У травні 2024 року WeChat повідомив, що майже вся інформація, розміщена на китайських порталах, блогах, форумах, сайтах соціальних мереж у період між 1995 та 2005 роками, більше недоступна[290].

Державною канцелярією у справах інтернету запроваджено обов'язкову реєстрацію користувачів (у 2010 роках введено обов'язкове підтвердження ПІБ користувачів онлайн-ігр), блокування сервісу WhatsApp та накладено заборону користування віртуальними приватними мережами, як VPN. На вимогу уряду КНР, місцеві державні провайдери (China Mobile, China Unicom и China Telecom) зобов'язані блокувати користувачам доступ до віртуальних приватних мереж [45].

Так, у нормативно-правовому акті КНР «Думка про поступову консолідацію відповідальності інтернет-платформ і сайтів з контролю за

контентом» наголошується про посилення контролю за акаунтами та необхідністю суворого виконання вимог, пов’язаних із ідентифікацією осіб, посиленням перевірок на відповідність правилам користувацьких угод використання нікнеймів та аватарів [291].

Тож доступ до інтернету та зміст контенту може істотно варіюватися залежно від підходів у правому регулюванні та правилах діяльність GAFA, які можуть деталізувати правила та умови надання доступу до певних об’єктів цифрового середовища та вимагати проходження реєстрації та ідентифікації тощо. Аналіз правового регулювання цифрових відносин у КНР свідчить, що інтернет може бути не лише вільним та відкритим, а й закритим, цензурованим та суворо контрольованим.

Означене демонструє, що здійснення прав на інформацію, права на свободу зібрання та право на вираження, доступ до державних адміністративних послуг у віддалених районах, доступ до медицини у КНР тісно пов’язаний із можливістю доступу до мережі «Інтернет» у сучасних реаліях, а в разі позбавлення особи права доступу до інтернету як санкції за вчинення правопорушення або злочину та видалення профілю (акаунта) фізичної особи неминуче призведе до позбавлення можливості реалізувати свої фундаментальні права, позбавлення доступу до товарів та послуг.

Вищезазначене дозволяє розмежовувати природно-правовий та позитивістський підходи до правого регулювання інтернету. Так, КНР послідовно запроваджується законодавство, спрямоване на посилення контролю за провайдерами та позбавленням доступу до мережі, обмеження доступу до західних сайтів та сервісів, цензурування та обмеження права вираження користувачів, а доступ до інтернету будується на ідеї, що воно є правом дарованим державою. У ліберальному підході до виникнення цифрової правоздатності покладена ідея фундаментального або природного характеру походження прав, обумовлених самою природою людини, її біосоціальною сутністю. Саме ця властивість служить засадою для визначення особистих

немайнових прав людини як фундаментальних, виникнення яких обумовлено лиши природною сутністю людини.

Уявляється, що доступ до інтернету можна пов’язувати з виникненням правоздатності фізичних осіб лише в демократичних, правових державах, де забезпечуються права людини та користувачі мають доступ до нього.

За аналогією із дієздатністю, цифрову дієздатність можна визначити як здатність своїми діями набувати та здійснювати права, створювати обов’язки та виконувати їх, нести юридичну відповідальність за свої дії чи бездіяльність у цифровому середовищі.

У науці висувається точка зору, за якою пропонується пов’язувати виникнення цифрової дієздатності з використанням цифрового профілю користувача [215, с. с. 58]. Слід визнати, що з моменту реєстрації та створення профілю (акаунта) на платформах державних адміністративних послуг, електронної комерції, соціальних мережах у більшості випадків у фізичної особи виникає здатність своїми діями здійснювати права та обов'язки на відповідній платформі в інтернеті. Залишається все менше цифрових сервісів у сфері електронної комерції, які надають послуги без обов’язкового створення акаунта (профілю).

Наразі попри те, що за законодавством момент виникнення повної дієздатності фізичної особи пов’язується із досягненням 18 річного віку, фактично фізичні особи отримують доступ до інтернету та здійснення окремих цивільних прав значно раніше досягнення віку, передбаченого законом для вчинення таких дій вже з моментом набуття технічних засобів доступу (смартфонів, комп’ютерів із доступом до мережі).

Окремі сайти, майданчики електронної комерції затребують формальне підтвердження досягнення особою віку під час отримання доступу до платформи в окремому вікні, в якому пропонується підтвердження досягнення особою повноліття. Надійність подібної перевірки ставиться під сумнів, адже користувач може формально підтвердити настання повноліття. Прикладом можна бути YouTube, який хоча в оновлених користувацьких угодах та політиці

конфіденційності зазначає про неможливість використання сервісу та запровадження окремого YouTube kids для малолітніх. Фактично малолітні особи можуть зареєструватися та навіть використовувати сервіс для продажу контенту на платформі [210, с. 7].

Наразі більшість додатків та сервісів пропонують користувачам використання електронних форм для заповнення та отримання відміни проведення транзакції та повернення грошей. Такі міри обумовлені випадками проведенням транзакцій неповнолітніми поза межами їх дієздатності. Google Play дозволяє користувачам відмінити проведену транзакцію протягом 48 годин та повернути витрачені гроші [304]. Наразі Google пропонує функцію «Запит на купівлю» в магазині додатків Play Market. Неповнолітні та інші члени сім'ї можуть надсилати запит на купівлю адміністратору (сімейній) групі, якому, у свою чергу, надані повноваження схвалювати або відхиляти проведення транзакції. Повідомлення про запит надходить адміністратору групи відразу після запиту на проведення покупки, з вимогою підтвердити списання грошей або відхилення транзакції. «Запит на покупку» не використовується в разі придбання електронних книг, товарів Google TV або при оформленні підписки. Схвалені транзакції зберігаються в «Історії замовлень» адміністратора (сімейної) групи.

Поряд із викладеним, малолітні особи мають доступ до значної кількості платних сервісів, де можуть використовуватися банківські картки, такі як Paypal, гаманці Qiwi, платіжні термінали та значна кількість безкоштовних сервісів, соціальних мереж, ігор тощо.

Фактично складається ситуація, що малолітні можуть вчиняти в інтернеті певні транзакції, розмір яких виходить за межі дрібних побутових правочинів, здійснювати особисті немайнові права на результати інтелектуальної, творчої діяльності, набувати права власності на цифрові активи [247], виходячи за межі часткової дієздатності. Власне, щоб стати користувачем соціальних мереж як Facebook, Instagram, Tiktok необхідно підписати користувальницьку угоду. У чинному законодавстві такий договір не передбачений, у науці висловлюються

різні точки зору щодо правової природи користувацької угоди. Висловлюються позиція, що цей договір є договором надання послуг, змішаним договором, договором sui generis [115, с. 62] або ліцензійним договором [184, с. 86].

Зазначимо, що всі спроби звести користувацьку угоду до договору про надання послугу не відповідає сутності такого договору, оскільки подібні послуги не мають альтернатив, користувач отримує доступ до нової реальності, де інші учасники мережі із застосуванням приладів створюють мережу, нову інформаційну, технічну та економічні системи, які з правової точки зору не є новим самостійним суб'єктом прав. Разом з цим, не вдаючись у глибинні дискусії з приводу природи користувальницької угоди, оскільки це не є предметом поточного дослідження, солідаризуємося з науковцями, які дотримуються позиції, що угоду Terms of Service слід вважати змішаним договором, який містить елементи декількох типів договорів, виходить за межі договору про надання послуг та ліцензійної угоди, передбачає положення про доступ до онлайн-платформи, обумовлює виникнення права власності на об'єкти, що знаходяться в акаунті, положенні про політику приватності, використання персональних даних тощо [115, с. 63].

Уявити ситуацію, при якій батьки укладали б користувацьку угоду від свого імені в інтересах дитини – майбутнього користувача досить складно, оскільки користування соціальною мережею передбачає спілкування з іншими користувачами, обговорення новин, відправка повідомлень, лайків саме від імені користувача. Практично користувацькі угоди ігрових платформ та соціальних мереж можуть укладатися неповнолітніми, малолітніми. Так на платформі багатокористувацьких ігор та програм Steam, покладають зобов'язання на користувачів гарантувати наявність повноваження укладання договору, а користувачі, які не досягли повнолітнього віку, гарантують, що отримали необхідний у відповідній законом формі дозвіл від батьків, опікунів або інших представників [251].

Як свідчить досвід, зазвичай користувацькі угоди не читають через формалізм викладеного матеріалу, а ні обізнані повнолітні, а ні діти та підлітки,

ставлячи таким чином користувача у вразливе становище. Користувацька угода Tiktok для користувачів не з США, ЄС, Швейцарії та Індії покладає обов'язок на користувачів регулярно переглядати Угоду для перевірки змін, та в разі не згоди негайно призупинити використання послуги[253]. Правоволоділець фактично може в будь-який час змінювати умови користувацької угоди стороною якої є малолітня особа, опублікувавши угоду зі змінами на сайті та запропонувавши користувачу приєднатися до угоди із внесеними змінами, які приймаються зазвичай автоматично [251]. Адже укладення користувацької угоди за технологією click-wrap, коли укладання договору відбувається шляхом проставлення галочки у віконцях або іншим аналогічними шляхом, передбачають механічні дії з боку користувача соціальних мережах, коли в цивільні правовідносин вступають малолітні фізичні особи, що не відповідає закріпленим нормам права.

Слід зазначити, що в ЄС Регламент ЄС 2016/679 передбачає обмеження, щодо односторонньої зміни правил обробки персональних даних, який вимагає отримання належної згоди на кожну обробку персональних даних.

З урахуванням викладеного, розглядаючи користувацьку угоду як договір змішаного типу з елементами різних договорів, реєстрації акаунта малолітніх у соціальних мережах не відповідає положенням ст. 31 ЦК України про часткову цивільну дієздатність фізичних осіб, які не досягли чотирнадцяти років, та їх право 1) самостійно вчиняти дрібні побутові правочини, які задовольняють побутові потреби особи, відповідає її фізичному, духовному чи соціальному розвитку та стосується предмета, який має невисоку вартість; 2) здійснювати особисті немайнові права на результати інтелектуальної, творчої діяльності, що охороняються законом.

Наразі можна стверджувати, що фізична особа самостійно приймає рішення щодо моменту настання власної цифрової дієздатності, якою є момент виникнення цифрового профілю особи. У науці висувається теза, що доцільно збереження класичного підходу до питання настання повної дієздатності та здійснення цифрових прав у мережі із досягненням віку та потребою

забезпечення механізму перевірки настання відповідного віку, за допомогою застосування цифрового ключа, на якому містяться дані про користувача, та який буде забезпечувати доступу до сайтів та послуг в мережі.

Означена теза виявляється дещо відірваною від фактичних виникаючих правовідносин, оскільки фізичні особи, які не досягли 14 років, беруть участь у багатофункціональних іграх, вступають у відносини в мережі з приводу отримання освітніх послуг, безоплатної психологічної та правової допомоги тощо. До того ж у віртуальному середовищі створюються або можуть бути придбані за реальні або віртуальні гроші ігрові предмети, віртуальна нерухомість та все те, що перебуває у віртуальному середовищі та в подальшому стає об'єктом правочинів [67, с. 24]. Користувацькі угоди таких соціальних мереж як Facebook [252], Instagram [254], передбачають можливість їх використання особами, які досягли 13 років або іншого мінімального віку, передбаченого згідно з законодавством відповідної держави. Фактично малолітні особи віком до чотирнадцяти років беруть участь у створенні та придбанні як об'єктів віртуальної власності та об'єктів права інтелектуальної власності у віртуальному середовищі.

У науці висловлюється точка зору, чи можна вважати створення фізичною особою цифрового профілю до досягнення нею повноліття – набуттям повної цивільної дієздатності фізичної особи або емансипацією у мережі «Інтернет». Дана позиція викликає сумніви, оскільки ст. 35 ЦК України передбачає надання повної цивільної дієздатності фізичній особі, яка досягла шістнадцяти років за наявності рішення органів опіки та піклування, за наявності письмової згоди батьків (усиновлювачів) або піклувальників, або за рішенням суду в разі зайняття трудовою діяльністю, підприємницькою діяльністю, якщо неповнолітня особа записана як батько або матір дитини. Тому визнавати початок використання мережі «Інтернет» набуттям повної цивільної дієздатності фізичної особи або емансипації є некоректним.

Як нам являється, то вирішення ситуації, яка фактично складається, коли малолітні укладають угоди, які виходять за межі мінімальної дієздатності,

покликані вирішити пропозиції, висунуті Н.О. Тищук, яка пропонує поділ малолітніх осіб на такі категорії або вікові групи: від народження до шести років – повністю недієздатні; від шести до десяти років – особи, які можуть самостійно звертатися про надання психологічної допомоги; мають право укладати правочини за допомогою персональної банківської картки під контролем батьків; від десяти до чотирнадцяти років – особи, які можуть самостійно здійснювати майнові права інтелектуальної власності, звертатися по безоплатну правову допомогу; бути безпосередніми активними учасниками деяких, пов'язаних із навчанням або іншим особистісним зростанням, майнових відносин, зокрема, відносин із надання освітніх послуг [210, с. 70].

За загальним правилом малолітні особи не несуть цивільно-правової відповідальності за завдану ними шкоду, з огляду на те, що вони не можуть повною мірою оцінювати свої дії і керувати ними, а тому не можуть визнаватися винними і нести відповідальність за правопорушення. Відповідальність за дії малолітніх покладається на їхніх батьків, усиновлювачів, опікунів, винних у нездійсненні належного нагляду за діями малолітнього чи неналежному вихованні дітей. Батьки, усиновлювачі, опікуни малолітніх можуть бути звільнені від відповідальності, якщо доведуть, що зобов'язання було порушене чи шкода заподіяна не з їхньої вини (ст. 33, 1178 ЦК). У свою чергу, у віртуальному середовищі малолітні особи можуть створювати та набувати права власності на цифрові об'єкти та об'єкти інтелектуальної власності під час участі в іграх.

Слід зазначити, що застосовування цифрового коду або ключа доступу, який містить дані про користувача, може надати можливість обмежувати доступ до певних державних, фінансових послуг для недієздатних або обмежено дієздатних осіб. Уявляється, що подібне обмеження доступу може бути застосовано щодо державних, адміністративних та фінансових послуг, у разі визнання особи обмежено дієздатною або недієздатною, яке відбувається за рішенням суду, за наслідками проведення медичної експертизи. У такому випадку, обмеження доступу до послуг може відбуватися автоматично, оскільки

дані про обмеження дієздатності або визнання фізичної особи недієздатною, мають завантажуватися до цифрового акаунта. Водночас обмеження фізичних осіб у придбанні товарів, послуг на сервісах електронної комерції, участі в іграх, де розрахунки можуть проводитися не лише за допомогою банківських карток, де поінформований банк має виконувати рішення, так і віртуальних грошей, уявляється вже більш складним.

З урахуванням вищезазначеного, можливість несення майнової відповідальності, деліктоздатності фізичними особами в інтернеті, має розглядатися із урахуванням означеної пропозиції, обумовленої віком та психологічним станом як умови притягнення до відповідальності, з урахуванням наявних технологій, які дозволяють ідентифікувати особу правопорушника, достатніх знань використання інформаційно-комунікаційних технологій та отримання доступу до них.

Питання притягнення відповідальної особи пов’язується із необхідністю її ідентифікації в мережі. Поряд із притягненням до кримінальної відповідальності винних осіб за порушення норм законодавства, користувацькі угоди містять положення про майнову шкоду учасників та можливість видалення облікового запису (акаунта) в разі порушення правил платформи. Так, Facebook передбачає можливість видалення або відключення облікового запису в разі серйозного та систематичного порушення користувацької угоди та політики мережі, норм спільноти, неодноразового порушення права на інтелектуальну власність інших людей або через інші юридичні обставини [252].

Відтак розвиток інформаційних технологій та мережі передбачає розгляд правосуб’єктності фізичної особи з тієї позиції, що права та обов’язки в цифровому середовищі виникають не лише у зв’язку з закріпленням певних прав та обов’язків у нормативно-правових актах, а розробкою та вдосконаленням технологій, коли сама мережа та цифрове середовище визначає, якими саме можливостями може користуватися людина в ньому. Наразі на правосуб’єктність особи в мережі впливають не лише такі категорії як громадянство, вік, психічне

здоров’я, а й технічні можливості, навички та знання, розвиток нових технологій, наявність електроенергії тощо.

Цивільна правоздатність фізичної особи припиняється в момент її смерті. Водночас в умовах цифровізації, коли змінюється ставлення особи до смерті під впливом новітніх технологій, пильну увагу викликають наслідки припинення правосуб’єктності фізичної особи в результаті фізичної смерті та припинення цифрової ідентичності фізичної особи в мережі «Інтернет». Підставою припинення правосуб’єктності фізичної особи є момент фізичної смерті особи, яку можна було б визнати актуальною й для цифрового середовища, проте особа внаслідок своєї діяльності в мережі залишає назавжди «цифрові сліди» у вигляді акаунтів (профілів) в соціальних мережах, валютних біржах, віртуальних іграх та різноманітних сайтах, які можуть мати майнову цінність, актуалізуючи питання правового врегулювання доступу до цифрової спадщини після смерті фізичної особи.

У зв’язку з тим, що внаслідок смерті фізичної особи відбувається правонаступництво, доцільно говорити про трансформацію цифрової ідентичності в силу переходу прав на цифрове майно, отримання доступу до акаунта (профілю) в інтернеті. У свою чергу, видалення акаунта та персональної інформації користувача, а з тим і здійснення фізичною особою своєї правоздатності та дієздатності може бути добровільним, за волевиявленням фізичної особи, та видалення профілю (акаунта) користувача може бути примусовим та застосовуватися як санкція за вчинення правопорушення законодавства за рішенням суду або порушення умов користувацької угоди за рішенням інтернет-сервісу.

Висловлюється думка, що на відміну від фізичного життя, в цифровому просторі неможливо зникнути навіть після смерті, окремі користувачі продовжують жити в інтернеті [60]. Начебто інтернет не пристосований для репрезентації фізичної смерті, що призвело до створення сайтів, цифрових кладовищ, меморіалів у пам’ять для вираження пошани та скорботи родичами та

друзями, що отримало назву танатотехнологій (з грецької танатос – смерть) [75, с. 205].

Поряд із трансформацією існуючого цифрового акаунта в цифровий меморіал, створення сторінки для висловлення скорботи, близькі покійного можуть запросити доступ до акаунта та цифрових речей [299, с. 20; 351, с. 93].

Інтернет-сервіси надають можливість створення цифрових меморіалів у пам'ять про масові трагедії, смерті або в пам'ять про конкретну загиблу людину, де друзі, родичі можуть в інтерактивному режимі залишати спогади та коментарі, вшанувати пам'ять загиблих [553, с. 34]. Наприклад, у мережі Твіттер є проєкт Remembrance Day на згадку про загиблих під час війни [768]. Facebook та Instagram надає можливість перетворювати сторінки користувачів у цифровий меморіал [2; 303; 566].

В умовах розвитку автоматизованих систем, які спеціалізуються на аналізі та обробці даних, компанії зацікавлені в розвитку цифрових меморіалів, оскільки збір, обробка та аналіз даних померлих осіб для навчання програм ШІ не потребує дотримання суворого законодавства про захист персональних даних та Регламент ЄС 2016/679 не поширюється на захист даних померлих осіб. До того користувачі, які відвідують цифрові меморіали, проводячи час в мережі, отримують рекламу, яка власне і є джерелом прибутку GAFA та решти компаній.

Слід розрізняти отримання доступу до акаунта після смерті особи для доступу до контенту, від трансформації існуючого цифрового акаунта та перетворення його в меморіал з метою вираження пошани до покійного, що не завжди забезпечує спадкоємцям доступ до цифрових активів, листування та всього контенту.

З урахування розглянутих вище підходів до правового регулювання мережі «Інтернет», слід констатувати, що в разі позбавлення доступу до мережі «Інтернет», особа фактично втрачає можливість здійснювати фундаментальні права. Повне відключення фізичної особи від мережі в державах із авторитарним підходом припинення функціонування мережі, відключення електроенергії, фактично позбавляє особу будь-яких прав та доступу до благ. Людина фактично

опинається виключеною від суспільства та цифрового середовища, за допомогою засобів якого проводиться оплата базових комунальних платежів, продуктів, товарів та послуг. Вказане дозволяє запропонувати категорію «цифрова смерть» для позначення випадків видалення акаунтів за життя користувача.

У широкому значенні термін «цифрова смерть» може застосовуватися як для позначення видалення акаунта, так і для створення спадкоємцями цифрових меморіалів на знак пошани померлого. Із видаленням акаунта, а з тим і персональних даних можливість здійснення правосуб'єктності фізичної особи може бути припинено за її власним бажанням на певному сайті. Слід зазначити, що у зв'язку з розвитком електронного урядування та можливістю згенерувати акаунт фізичної особи в певних державних інформаційних системах, використання добровільного видалення акаунтів користувачем може застосовуватися виключно у приватних інформаційних систем.

Із питанням цифрової смерті тісно пов'язано отримання доступу до даних користувача в мережі після його смерті, яке стосується здійснення спадкових прав фізичної особи, отримання доступу до цифрових об'єктів та формування режиму майна фізичної особи після смерті. Слід констатувати, що підходи до правового регулювання здійснення спадкових прав на цифрові об'єкти після смерті фізичної особи в США та державах ЄС є досить різними.

Як було вже з'ясовано, користувач може заповнити спеціальну форму для розпорядження своїм акаунтом на випадок смерті, якщо платформа передбачає такий функціонал [199]. Наразі в умовах поширення управління майном особи на випадок смерті [227, с. 129; 245, с. 848], з'являються платформи, які надають послуги з управління цифровими речами та «цифровою спадщиною» в разі залишення спадкодавцем відповідних розпоряджень на випадок смерті [778]. Такі компанії беруть на себе обов'язки виконувати розпорядження спадкодавця, зроблені ним на випадок його смерті [661, с. 385].

Визначення обсягу даних та об'єктів щодо яких може бути наданий доступ після смерті спадкодавця в мережі може актуалізувати питання співвідношення

цифрового розпорядження на платформі, поряд із паперовим нотаріально засвідченим заповітом. У США дотримуються пріоритету розпорядження в електронній формі вчиненого на платформі поряд із заповітом. Відповідно до ст. 2701-2712 Акта про зберігання повідомлень у складі Акта про захист права на приватне життя компаніям заборонено розкривати зміст акаунта та електронних повідомлень третім особам та органам державної влади без їх законної згоди відправника повідомлень, одержувача або користувача. Акт про зберігання повідомлень передбачає відповідальність за навмисний доступ до електронних повідомлень без дозволу користувача або за навмисне зловживання доступом, запобігаючи доступу до повідомлень третім особам. Якщо спадкоємці або інші особи звертаються для отримання доступу до акаунта, платформи можуть відмовити спадкоємцям із посиланням на даний Акт [500]. Означена норма свідчить про безумовний пріоритет волі користувача щодо доступу до його облікового запису. Саме на дане положення посилалися суди, для обґрунтування відмови в наданні доступу спадкоємцям до вмісту акаунта у справі загиблого військового Дж. Еллсворта проти Yahoo! у 2004 році [877].

Винятки, передбачені у ст. 2702 Акта, вплинули на формування підходу для надання доступу до цифрових активів в США. За твердженням Н. Кан, Акт про зберігання повідомлень, прийнятий Конгресом у 1986 році, не відповідав вимогам для вступу у спадщину в цифрову епоху, а переважно стосувався забезпечення приватності від хакерських атак та шпигунства державних органів за громадянами[359, с. 1698]. А спрогнозувати вплив бурхливого розвитку технологій у вісімдесяти роки Конгрес не міг, як і передбачити онлайн-банкінг, доступний американським споживачам з 1995 року [682].

Водночас застосування цього Акта для регулювання доступу до цифрових об’єктів після смерті спадкодавця зазнало критики, тому для врегулювання управління цифровими об’єктами в мережі та одноманітного застосування законодавства в різних штатах у 2014 році Комісія з уніфікованого права США оприлюднила первісний варіант Єдиного закону про довірчий доступ до цифрових активів, з метою усунення перешкод для доступу фідуціара до

електронних листувань [823]. Проєкт закону передбачав надання особистим представникам права доступу до змісту електронних повідомлень, якщо тільки спадкодавець ясно не передбачив протилежне. Проте через супротив GAFAM через виникнення ризику порушення законодавства про приватність в окремих штатах, було прийнято переглянутий варіант Єдиного закону про довірчий доступ до цифрових активів США. Переглянутий Єдиний закон вимагає, щоб особистий представник надав згоду користувача на розкриття акаунта для отримання доступу, тому нерозголошення є правилом за замовчуванням, якщо померлий не висловив своєї волі. З 2015 року більшість штатів прийняли законодавство стосовно довірчого доступу до цифрових активів, яке передбачає законну згоду померлого на розкриття даних.

Положення про надання доступу до інформації особи в мережі «Інтернет» викладено в Єдиному законі про довірчий доступ до цифрових активів, який передбачає безумовний пріоритет розпорядження цифровими речами, залишеними на платформі [769]. У 2015 році було внесені зміни до Єдиного закону про довірчий доступ до цифрових активів, які передбачили систему пріоритетів розпорядження акаунтом та його вмісту. Єдиний Закон у переглянутій версії передбачив пріоритет спеціального розпорядження на цифровій платформі, поряд із заповітом, трастом, довіреністю та іншими розпорядженнями. У разі відсутності електронного розпорядження та заповіту, застосовуються загальні умови користування акаунтом. Таке положення вочевидь знижує витрати користувача на оформлення розпоряджень на випадок смерті, відносно цифрових об’єктів. Водночас залишення електронного розпорядження на платформі та заповіту в письмовій формі може порушувати невирішені питання з’ясування черговості вираження останньої волі. Якщо порівнювати з письмовим документом, посвідченим нотаріально, то залишення електронної достовірності особи, яка залишила розродження на платформі, може бути перевірений лише платформою за допомогою введення логіну, пароля та інших можливих засобів автентифікації. Порід із цим, очевидною перевагою

цифрового розпорядження для користувача є мінімізація витрат щодо розпорядження майном на випадок смерті.

До того ж, існуючий пріоритет електронної форми не дозволяє впевнитися в тому, що саме користувач склав та залишив розпорядження про доступ до свого акаунта на випадок смерті. Адже розпорядження в електронній формі ґрунтується лише на презумпції, що воно складено самим користувачем, який володіє паролем та логіном та зобов'язаний вжити заходи, щоб забезпечити їх конфіденційність. З іншого боку, безумовний пріоритет електронного розпорядження мінімізує витрати на встановлення та виконання волі користувача на платформі.

Положення Єдиного закону дотримуються положень нейтральності активів [625, с. 644; 246, с. 41]. За даною концепцією, якщо спадкодавцем залишено розпорядження на платформі, фідуціар, який має доступ до матеріальних активів померлого за законом отримує такий же доступ до акаунтів (всього вмісту облікового запису), які існують у цифровій формі, що надає йому право контролювати та копіювати цифрові об'єкти, такі як фото, листування, які розміщені на акаунті.

У більш пізній справі Аджемяна проти Yahoo!, де брат та сестра Аджемяна у 2006 році звернулися до Суду зі спадкових та сімейних справ для отримання доступу до акаунта електронної пошти загиблого, обґрунтовували свою позицію тим, що акаунт є частиною майна покійного, до якого вони мають право доступу як управителі спадкового майна, призначені судом. Верховний суд США у 2018 році, який відхилив посилання Yahoo!, залишивши остаточним рішення Верховного суду штату Массачусетс від 17.10.2017 року, що особисті представники можуть надавати законну згоду від імені померлого на оприлюднення вмісту облікового запису електронної пошти Yahoo [393; 730].

Із викладеного можна зробити висновок, що судова практика США визнає значущість акаунтів для управління та охорони спадщини, проте цифрові об'єкти не виокремлюються у самостійні об'єкти спадщини. Судова практика визнає право за спадкоємцями на доступ до акаунта, водночас дотримується ідеї

управління акаунтом після смерті особи, та надання доступу для виконання певних задач без заміни спадкодавця у відносинах із провайдером та без передачі прав та обов'язків спадкоємцям за користувацькою угодою.

Відтак, якщо національне законодавство не передбачає спеціальних норм щодо порядку отримання доступу до цифрових об'єктів, можливість отримання доступу до цифрових об'єктів після смерті спадкодавця визначається користувацькою угодою між користувачем та платформою. Якщо жодних розпоряджень на платформі та заповіті не залишено, особи, зацікавлені отримати доступ до акаунта можуть звернутися до суду.

Аналогічно рішенню у справі Джона Аджемяна у США, у 2012 році в Німеччині тривав спір між батьками померлої п'ятнадцятирічної дівчинки та Facebook, стосовно переходу до спадкоємців користувача прав на обліковий запис у соціальній мережі та способу надання доступу до такого облікового запису. Переглянувши рішення попередніх інстанцій, Федеральний Верховний суд у 2020 році прийняв рішення, що позивачам має бути наданий доступ до контенту, що міститься в акаунті користувача та доступ до облікового запису користувача в такому вигляді, як мав доступ власник акаунта. Суд аргументував рішення тим, що права та обов'язки за користувацькою угодою переходять до спадкоємців у порядку універсального правонаступництва, відповідно до ст. 1922(1) ЦК Німеччини за користувацькою угодою до спадкоємців за законом [356; 526, с. 5].

У даній справі заслуговує на увагу, що Суд зазначив, що інші користувачі Facebook не можуть обґрунтовано очікувати, що їх повідомлення не будуть доступні третім особам та відхилив твердження Facebook, на які він посилався, про необхідність захисту приватного життя та таємницю листування загиблої дівчинки. Суд підкреслив, що законодавча вимога щодо захисту таємниці телекомунікацій, передбачена ст. 88 Закону Німеччини про телекомунікації, не суперечить праву спадкоємців вимагати доступу до інформації через те, що спадкоємці користувача не визнаються як треті особи в розумінні таємниці телекомунікацій.

Крім того, Регламент ЄС 2016/679 не забороняє право спадкоємців на доступ до облікового запису померлого користувача у Facebook, а законодавство про захист персональних даних не застосовується до померлих осіб. На думку Суду, обробка персональних даних третіх осіб, з яким спілкувався спадкодавець, була дозволена відповідно до п. b абз. 1 ст. 6 Регламенту ЄС 2016/679, оскільки це було необхідно для захисту даних спадкодавця, а також для забезпечення його безпеки; необхідно для виконання договірних зобов'язань перед особою, з якою спілкувався спадкодавець (незалежно від смерті власника облікового запису) («необхідно для виконання договору») та необхідно було дотриматись законних переважних інтересів спадкоємців.

Зазначена справа порушує питання можливості здійснення спадкоємцями та уповноваженими особами прав на підставі користувацької угоди від імені померлої особи, отримання доступу до акаунта, який включає особисте листування спадкодавця із третіми особами, таким чином нехтуючи таємницю листування померлого та особистими немайновими правами, як складовими цифрової смерті. Прийняте рішення залишається дискусійним [544, с. 1195]. За твердженням Т. Мік та К. Сейн застосування принципу універсального правонаступництва, притаманного державам романо-германської правової системи, мало істотне значення для прийняття рішення Федеральним Верховним судом Німеччини[672, с. 117]. Дж. Буйтелар, навіть ставить питання щодо захисту приватності після смерті особи, наділення суб'єктів правом недоторканності приватного життя після смерті. Ставить питання, кому поряд зі спадкоємцями, можуть надаватися повноваження контролювати та припиняти незаконне використання об'єктів у мережі після смерті спадкодавця [353, с. 130].

Дж. Лі стверджує, що цифрові активи надають високий рівень доступу до персональної інформації, що недоступна фізичним активам як за характером, так і за обсягом, що цифрові активи часто надають доступ до прямих трансляцій у режимі реального часу, в яких беруть участь користувачі акаунтів, і, таким чином, надаючи доступ до цифрових активів третіх осіб. З метою захисту приватного життя всіх користувачів, як живих, так і померлих, довірчий доступ

до акаунтів має бути обмежений лише доступом до акаунта спадкодавця для реалізації певних задач ознайомлення. Проте управитель не має замінювати користувача у правовідносинах із платформою [625, с. 644].

К.Г. Некіт звертає увагу на те, що позиція Т. Міка та К. Сейн є хибною, оскільки особисті договори, зазвичай, не підлягають універсальному правонаступництву згідно зі спадковим правом. У свою чергу, користувачі платформами соціальних мереж, переважно, укладають саме особисті договори. Крім того, умовами користувацьких угод, зазвичай, передбачено положення, що користування акаунтом надається конкретно визначеному користувачу та заборонено надання доступу до акаунта третім особам, якщо прямо не передбачено зворотне[690, с. 297]. Відповідно до положень українського законодавства, не можна успадкувати права та обов'язки, які нерозривно пов'язані з особою спадкодавця та особисті немайнові права [121]. Ст. 1219 ЦК України передбачено, що не входять до складу спадщини права та обов'язки, що нерозривно пов'язані з особою спадкоємця, зокрема особисті немайнові права. Натомість право на створення акаунта надається саме конкретно визначеній особі, яка надала свої персональні дані під час реєстрації на платформі. Відповідно можливість доступу до акаунта не може передаватися в порядку спадкування. Як зазначається у ст. 270 ЦК України право на таємницю листування відноситься до одного з видів особистих немайнових прав поряд із правом на життя, правом на охорону здоров'я, правом на безпечне для життя і здоров'я довкілля, правом на свободу та особисту недоторканність, правом на недоторканність особистого і сімейного життя, правом на повагу до гідності та честі та іншими правами. Для можливості спадкування в такому разі мають значення не лише функціональні можливості акаунта, а й є те, що акаунт у соціальній мережі може відображати особисті вподобання та бачення померлої особи як особистий щоденник, а тому порушувати особисті немайнові права померлої особи, яка могла бажати залишити своє особисте листування в таємниці.

З урахуванням особистісної природи акаунтів у мережі, науковці припускають, що оптимальним механізмом для забезпечення надання доступу до акаунтів у разі смерті, має стати призначення цифрового виконавця для управління цифровим майном особи в мережі після смерті. Такого виконавця не слід ототожнювати із особистим представником [690, с. 297].

Якщо договір про відкриття акаунта в соціальній мережі визнавати договірним зобов'язанням, на відміну, наприклад, від членства в асоціації, яке не переходить до спадкоємця, постає питання надійності виключення акаунта зі спадкової маси, за умовами користувацької угоди. Facebook надає можливість відповідно до умов користувацької угоди призначити спадкоємців, що покликано виключенням акаунта з об'єктів спадкування. Водночас законодавство наразі не містить положень щодо спадкування акаунтів, тому постає питання, чи буде достатньо користувачу обрати положення опцію про виключення акаунта з об'єктів спадкування, щоб запобігти передачі своїх даних третім особам.

Тож питання цифрової смерті та отримання доступу до цифрових об'єктів актуалізують питання відносно співвідношення між нотаріально посвідченим заповітом та електронним розпорядженням. У цьому аспекті може бути встановлено в законодавстві пріоритет нотаріальної форми заповіту або встановлено рівнозначність між електронним розпорядженням та нотаріальною формою заповіту, що актуалізує встановлення часу прийняття електронного розпорядження та нотаріального заповіту.

При формуванні засад правового регулювання цифрової смерті, необхідно брати до уваги особливість електронної форми розпорядження на випадок смерті, яка залишається на цифровій платформі та полягає в заповненні окремої спеціальної форми в межах облікового запису (акаунта), користувача, поряд із укладенням користувальницької угоди. З огляду українського законодавства, таке електронне розпорядження є електронним документом, підписаним простим електронним підписом, а можливість підписання електронного розпорядження за допомогою КЕП, цифрові платформи не передбачають.

Можна підсумувати, що держави можуть обирати різні напрями правового регулювання доступу до майна на випадок смерті. Відповідно до першого підходу, забезпечується пріоритет дотримання особистих немайнових прав та інтересів спадкодавця, що передбачає певні обмеження доступу до акаунта, листування та особистих даних після смерті користувача. Другий підхід передбачає, правове регулювання доступу до цифрових об'єктів на випадок смерті, засноване на користувацькій угоді, якщо у законодавстві не містяться спеціальні правові норми щодо цифрових розпоряджень. Такий підхід актуалізує питання можливості спадкування прав та обов'язків спадкодавця за користувацькою угодою, та питання, в якому вигляді платформа має надати доступ до акаунта, якщо це соціальна мережа. Адже відносини між спадкодавцем та платформою носять довірчий характер.

Якщо відповідно до положень про спадкування за відсутності прямого волевиявлення спадкодавця, об'єкти спадщини перерозподіляється між спадкоємцями відповідної черги, в разі смерті та відсутності прямого волевиявлення спадкодавця, платформи обирають шлях мінімального розкриття даних, надання доступу до даних або не розкриття даних, що відображає судова практика США. Лише наполегливі та довготривалі судові спори спадкоємців із платформами здатні змінити ситуацію на користь спадкоємців.

Підсумовуючи викладене, зазначаємо, що здійснення прав на доступ до цифрових об'єктів після смерті спадкодавця ставить такі проблемні питання, як можливість розпорядження всіма даними фізичної особи в мережі та проблему щодо форми розпорядження залишеного на платформі особою.

Торкаючись питання правового регулювання цифрової смерті та термінології, передбаченої законодавством України, слід зазначити, що заповнена форма зі спеціальним розпорядженням на платформі є електронним документом, який підписується електронним підписом відповідно до ст. 12 Закону України «Про електронну комерцію» [154].

На сьогоднішній день Проєкт Закону України «Про внесення змін до Цивільного кодексу України щодо унормування питання прийняття спадщини,

спадкодавець якої перебуває за кордоном» доповнює ст. 1297 ЦК України, яка передбачає можливість дистанційного оформлення заяви в паперовій формі рекомендованим листом або в електронній формі через Єдиний держаний вебпортал електронних послуг, який не передбачає положень стосовно порядку доступу спадкоємців до цифрових об'єкт після смерті їх власника [143].

Згідно з Законом України «Про віртуальні активи» [146], він не передбачає особливості спадкування цифрових об'єктів та речей та зазначає, що порядок вступу у спадщина щодо таких об'єктів має відбуватися відповідно до положень ЦК України. Як було розглянуто вище, однією із перешкод для отримання доступу до акаунтів може стати втрата паролей, тож доцільно складати заповіт із зазначенням цифрових об'єктів. Припускається, що в разі смерті спадкодавця, нотаріус або спадкоємець мають звернутися із заявою до служби клієнтської підтримки платформи зі: свідоцтвом про смерть користувача; документами, що підтверджують особу спадкодавця та спадкоємця; свідоцтвом про право на спадщину, посвідчене нотаріусом. За результатами розгляду документів платформа (криптовалютна біржа), мають підтвердити права на спадкове майно та зарахувати цифрові активи на рахунок спадкоємці [200].

Поряд із цим, спадкодавець може залишити спеціальні розпорядження із зазначенням конкретних осіб в електронному розпорядженні на платформі на випадок смерті, якщо функціонал платформи передбачає таку можливість, що переважно стосується соціальних мереж. Означений підхід порушує актуальність питання щодо можливості спадкування прав та обов'язків спадкодавця за користувацькою угодою, або способів надання доступу до акаунта, якщо це соціальна мережа. Адже відносини між спадкодавцем та платформою носять довірчий характер. У подальшому можна припустити вірогідність виникнення суперечливих питань щодо пріоритетності, в разі залишення цифрового розпорядження на платформі та нотаріально засвідченого заповіту, де спадкоємцями зазначені різні особи, як було зазначено вище. У такому випадку в законодавстві доцільно врегулювати питання, чи входить

цифрове майно до складу спадщини. Тому вважаємо доцільним доповнити ЦК України статтею 1228-1 «Спадкування цифрового майна» таким змістом:

1. Заповідач може залишити розпорядження на цифровій платформі або в заповіті, в якому призначити особу, до якої має перейти право власності на цифрове майно в разі його смерті.

2. Договірні розпорядження щодо цифрового майна залишені заповідачем на випадок смерті мають пріоритет над заповітом складеним на те саме майно.

3. Доступ до особистого листування, щоденників може бути надано спадкоємцям, якщо спадкодавець залишив пряме розпорядження про розкриття таких даних у розпорядженні або заповіті.

4. У випадку, якщо спадкодавець не залишив розпорядження щодо цифрового майна в заповіті або на цифровій платформі, спадкування такого майна відбувається відповідно до закону або користувацької угоди.

Слід зазначити, підхід до концепції «цифрової спадщини» закріплений у законодавстві Франції. У формуванні підходу до спадкування та отримання доступу до цифрових об'єктів після смерті фізичної особи взято до уваги, що цифрова ідентичність розглядається у вузькому та широкому значенні. Відповідно до Закону Франції Про інформаційні технології, документи та свободи [628], передбачено режим доступу та розпорядження даними після смерті фізичної особи, який надає право спадкоємцю залишити розпорядження (директиву), що може бути загальним – передбачати право на доступ до усіх даних після смерті особи в мережі, та спеціальним – встановлювати волю особи на розпорядження конкретними цифровими об'єктами. Спеціальні розпорядження користувач реєструє та залишає на цифровій платформі на випадок смерті, з урахуванням функціоналу та не вимагає звернення до будь-яких третіх осіб. Якщо спадкодавець не залишив спеціальних розпоряджень, спадкоємці можуть вимагати доступ до акаунта або видалення акаунта.

Поряд із спеціальними розпорядженнями, згідно зі ст. 40-1 Закону Франції про захист даних і свобод від 17.12.2015, передбачено право особи залишити

загальні розпорядження на випадок смерті (які стосуються усіх акаунтів, які фізична особа створила та залишила в мережі), підлягають реєстрації уповноваженим сертифікованим фахівцем CNIL – який забезпечує конфіденційність при зборі, обробці та використанні даних) [631]. Спадкодавець може призначити виконавця розпоряджень, уповноваженого вимагати виконання розпоряджень та останньої волі спадкодавця від цифрових платформ. У разі смерті призначеної особи, його спадкоємці мають право прийняти розпорядження спадкодавця та звертатися із запитами про виконання до уповноважених платформ. Посилання на загальні розпорядження підлягають реєстрації в єдиному реєстрі загальних розпоряджень, ведення якого має бути визначено законодавством.

Перепонами для успішної реалізації вищезгаданих положень є відсутність порядку ведення реєстру загальних розпоряджень. Французькі нотаріуси у 2017 році на Конгресі Нотаріусів пропонували передати повноваження із реєстрації розпоряджень цифровими об'єктами нотаріусам, яке наразі не отримало законодавчого закріплення [634]. Крім того, отримання доступу та спадкування загальних розпоряджень цифрової ідентичності потребує подальших технічних розробок, їх впровадження, які б дозволили б об'єднання розрізнених облікових записів у єдиному профілі. Складнощі постають через те, що користувачі мають велику кількість акаунтів на різних платформах та соціальних мережах, не завжди пам'ятають паролі доступу від них, нехтуючи сервісами зберігання ключів, розпорядження на випадок смерті залишають на окремих сервісах. Тому встановити всі сервіси, на яких особа була зареєстрована, якими користувалася за життя та мала акаунти з цифровими активами, які мають якусь майнову або немайнову цінність, є досить складним. Подібні правові проблеми, що виникають відносно забезпечення доступу до акаунтів та цифрового майна після смерті фізичної особи, має допомогти вирішити технологія єдиної суверенної цифрової ідентичності на базі блокчейн, яка має об'єднати розрізнені акаунти в єдиній децентралізованій системі[296]. Така ситуація актуалізує питання

визначення обсягу даних, до яких спадкоємці можуть отримати доступ після смерті спадкодавця, яке вимагає технологічних удосконалень.

Досвід Франції свідчить, що доступ до загальних розпоряджень після смерті особи та реалізації широкого підходу до цифрової ідентичності супроводжується практичними та технологічними перешкодами, що потребують додаткового регулювання. Поряд із проблемою отримання доступу до даних акаунтів на вимогу спадкоємців, з огляду норми про загальні розпорядження, постає проблема, знайти та встановити всі платформи та соціальні мережі, де користувач створив акаунти протягом життя.

Як зазначають хорватські науковці Р. Вучковіч, І. Канцеляк, спадкоємці можуть не знати про залишені цифрові розпорядження та цифрове майно померлого. Науковці розмірковують, що користувач може залишити документ із переліком своїх облікових записів разом з іменами та паролями, та передати на зберігання нотаріусу на випадок смерті. Проте залишаються побоювання про розкриття паролей, крім того, паролі рекомендовано періодично змінювати, тому такий документ може втратити свою актуальність [847, с. 725]. Ми вважаємо, що така пропозиція є застарілою з огляду на розвиток сервісів, які надають послуги з управління цифровим майном на випадок смерті.

У разі застосування технології суверенної цифрової ідентичності на базі децентралізованої системи блокчейн, розпорядження користувача щодо долі його майна на випадок смерті, зможе поширюватись на пов'язані акаунти, що дозволить отримувати доступ та управляти доступом до даних фізичної особи.

Підсумовуючи викладене, з урахуванням розглянутих підходів щодо надання доступу до майна фізичної особи в разі смерті, можна стверджувати про формування двох підходів. Відповідно до першого, дотримуються особисті немайнові права померлої особи, надаючи їй останню волю щодо визначення ступеня доступу до її даних, при цьому права спадкоємців на доступ до даних, які мають майнову цінність, залишається певною мірою обмеженими волею спадкодавця, та другий підхід, який переважно бере до уваги інтереси

спадкоємців та інших осіб, які управляють майном, не приділяючи уваги автономії волі спадкодавця.

3.2. Зміст цивільної правоздатності фізичної особи в мережі «Інтернет»

У часи правових трансформацій, підходи законодавця до визначення правоздатності зазнавали істотних змін з огляду на пануючу доктрину в державі. Адже зміст правосуб'єктності фізичної особи та комплекс прав та обов'язків людини є динамічним, обумовлений розвитком суспільства, який вносить зміни відповідно до її потреб, у тому числі у визначенні прав, наданих всім особам. З огляду на бурхливу цифровізацію, сьогоднішня система прав людини значно розширилася з часу прийняття ЗДПЛ, через появу нових прав в інтернеті, що впливає на зміни змісту правосуб'єктності фізичної особи в мережі «Інтернет».

З погляду М. Одело та С. Кавандолі, через мінливий характер суспільства, права людини переживають постійну еволюцію, обумовлену розв'язанням викликів [695, с. 5]. Права людини будучи ситуативними, формуються в суспільстві в певний момент часу. Р. Браунсворд та М. Гудвін стверджують, що технологічні розробки призведуть до створення нових прав людини, серед яких називають: право на генетичну недоторканність приватного життя, право на унікальність особистості, а також право на доступ до інтернету тощо [350, с. 50].

Цифрові зміни в суспільстві вимагають теоретичного переосмислення традиційних юридичних понять, формулювання правового механізму регулювання, здійснення та захисту суб'єктивних прав та обов'язків особи в цифровому середовищі. Цифрова трансформація безпосередньо впливає на здійснення правосуб'єктності особи на національному та міжнародному рівнях, сприяючі появі та зміні прав та обов'язків особи як учасника всесвітнього інформаційного цифрового простору.

Основні засади функціонування інформаційного суспільства викладені в таких актах як: Окінавська глобальна хартія інформаційного суспільства, прийнятій у 2000 році[697], Декларація принципів «Побудови інформаційного суспільства: глобальної задачі нового тисячолітті», 2003 року [467], Туніській програмі для інформаційного суспільства, прийнятій у 2005 році [837] тощо.

Про необхідність розвитку інформаційного суспільства, створення цілісної системи законодавства, його гармонізації з нормами міжнародного права з питань розвитку інформаційного суспільства наголошується в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 р. № 537-V [161].

Тож поряд із традиційними особистими немайновими та майновими правами особи, які закріплені в Конституції, ЦК та законодавстві формується покоління прав, обумовлених функціонуванням новітніх технологій та поширенням інтернету. Відтак за твердженням Дж. Коколі, технологічні інновації не лише вимагають перегляду та інтерпретації традиційних прав особи, але й обґрунтовують появу нових категорій, які можуть бути визначені як sui generis покоління цифрових прав [437, с. 226].

Слід констатувати відсутність єдності у використанні термінології прав у мережі «Інтернет». В англомовних джерелах трапляється використання таких термінів для позначення прав у мережі як: інформаційні (комунікаційні), цифрові[437, с. 226], інтернет права, права на комунікацію, свобода з'єднання з будь-якою особою в будь-який час, у будь-кому місці, для будь-якої мети [740, с. 12]. Означені терміни в літературі трапляються переважно як синоніми, а подекуди акцентується увага на певних властивостях зазначених прав.

На думку Д. Коколі, такі терміни як інформаційні та комунікаційні права акцентують увагу на свободі отримання та поширення інформації, участі у процесі комунікації та необов'язково пов'язані із використаним новітніх технологій, можуть бути здійсненні у фізичному світі та в мережі, боротьба за їх міжнародне визнання почалася до поширення інтернету. У той же час застування терміна «віртуальний» на позначення прав, може свідчити про «нереальні» властивості прав, що вочевидь є некоректними. Застосування «мережеві» або «інтернет» на позначеня прав обмежує сферу застосування вказівкою на доступ до мережі, водночас сучасні технології не обмежуються доступом до інтернет-мережі. За таких умов науковець відстоює позицію застосування більш загальної

категорії як: «право на доступ до сучасних та технологічних досягнень та використання переваг, що випливають з них» [437, с. 226].

Тому найбільш прийнятним є термін «цифрові права». Н.В. Верлос, К.О. Калаченкова, Т.В. Михайліна називають такі шляхи правового регулювання цифрових прав: конституціоналізацію цифрових прав, відповідно до якої вносяться зміни до Конституції; цифровізація конституційних прав, відповідно до якої існуючі права набувають оновленого тлумачення або врегулювання практики ЄСПЛ або профільному законодавстві, органами конституційної юрисдикції [22, с. 130; 591, с. 93].

Резолюція Генеральної Асамблеї ООН від 25.09.2015 № A/ RES/70/1 визначає «Порядок денний у сфері сталого розвитку на період до 2030 року», де в межах цілі «Створення стійкої інфраструктури, сприяння всеосяжній та стійкій індустріалізації та інноваціям» передбачено істотне розширення доступу до інформаційно-комунікаційних технологій та прагнення забезпечити загальний та недорогий доступ до інтернету в найменш розвинених державах до 2020 року».

Для об’єднання в єдиному документі прав громадян та принципів правового регулювання, які наразі викладені в різних директивах, правилах та конвенціях ЕС, що ускладнюють їх застосування споживачами та постачальниками послуг, у 2013 році Європейська комісія опублікувала Кодекс онлайн-прав ЄС, який є збіркою основних прав у галузі електронних комунікацій, електронної комерції та захисту прав споживачів в інтернеті в ЄС. Кодекс не є актом прямої дії, однак права та принципи, викладені в ньому, підлягають виконанню відповідно до правових актів ЄС. Кодекс передбачає, що кожна особа в ЄС повинна мати можливість отримати доступ до мінімальної низки електронних послуг гарної якості за доступною ціною на основі принципу «універсального обслуговування» [438].

Коаліція з прав людини та принципів інтернету запропонувала використання нині гарантованих права людини в інтернет-середовищі,

розробила та прийняла Хартію прав людини і принципів для інтернету у 2006 році, в якій називаються такі права людини:

- право на доступ до інтернету (ст. 26 ЗДПЛ) та право на недискримінаційний доступ, використання та управління інтернетом. Дане право охоплює низку правомочностей, пов'язаних з участю в управлінні інтернетом: правом на володіння навичками користувача; право на розробку, володіння контентом та пристроями; право на доступ до інфраструктури та мереж, право на управління інтернетом; рівність у доступі до мережі, в тому числі осіб із інвалідністю (гарантії якості обслуговування, свобода вибору використання систем та програмного забезпечення, забезпечення підключення, мережевий нейтралітет;

- право на свободу вираження думок та інформації в мережі (за ст. 18-20 ЗДПЛ), що передбачає свободу висловлювання та думки, яка включає свободу від цензури в інтернеті, свободу участі в онлайн-зібраннях, участь в онлайн-протестах, недопущення використання мови ворожнечі;

- право на доступ до знань (ст. 27 ЗДПЛ), що гарантує право на участь у культурно-соціальному та науковому прогресі; право на свободу доступу до інформації в мережі; та право на інформацію про інтернет та права людини;

- право на безоплатне відкрите програмне забезпечення та технології (ст. 27 ЗДПЛ), що містить право на створення та поширення програмного забезпечення з відкритим кодом; право на отримання переваг від використання контенту тощо;

- право на конфіденційність, свободу від стеження та шифрування даних (ст. 12 ЗДПЛ), що гарантує право на недоторканність особистого життя: право на захист даних, свободу від стеження; використання шифрування; налаштування конфіденційності; стандарти конфіденційності та цілісності ІТ-систем; захист віртуальної особистості; право зберігати анонімність та використовувати шифрування; свободу від стеження та наклепів; право на захист персональних даних (включає обов'язки суб'єктів, які збирають дані, мінімальні

стандарти обробки використання персональних даних, моніторинг діяльності компаній незалежними органами із захисту даних) [815].

Хартія також приділяє увагу таким правам в Інтернеті як: право на свободу та безпеку в інтернеті (захист від усіх форм злочинності); право на розвиток за допомогою використання інтернету (екологічна стійкість та подолання бідності); свобода віросповідання та переконань; право на доступ до культуру та знань (право на участь у культурному житті громади, різноманітті мов та культур, право користуватися власною мовою, використання вільного програмного забезпечення); право дітей на доступ до мережі та їх захист; право на працю в мережі (повага до прав працівників, забезпечення доступу до інтернету на робочому місці, рівний доступ до електронних послуг та участь в електронному урядуванні); захист прав споживачів в інтернеті (доступ до онлайн-контенту, пов'язаного зі здоров'ям та соціальними послугами в інтернеті); справедливий судовий розгляд за дії вчиненні в інтернеті (право на судовий захист та справедливий суд); право на соціальний та міжнародний порядок у інтернеті (ефективне управління інтернетом для дотримання прав людини, багатомовність і плюралізм в мережі); забезпечення дотримання обов'язків та несення відповідальності за порушення прав в мережі.

Тож Хартія прав людини і принципів для інтернету охоплює всі права людини, спираючись на ЗДПЛ та інші пакти, які становлять Міжнародний білль про права людини ООН, у тому числі називає права, розвиток яких обумовлений виключно появою інформаційно-комунікаційних технологій та мережею.

Дискусії з приводу здійснення фундаментальних прав людини в умовах цифровізації відображають уявлення про зростання загрози правам через нові системи контролю, збору персональних даних, профілюванню, зростаючу роль провідних інтернет-компаній та їх монополізації.

Скандали довкола Є. Сноудена, Дж. Ассанжа, Кембридж Аналітики та інших цифрових платформ, безсумнівно вплинули на проблеми приватності та цифрових прав, та привернули до них увагу. На додаток до широкої дискусії щодо цифрових прав, правозахисні організації зосередили зусилля на

документуванні та просуванні діяльності із недопущення порушення та обмеження прав суб'єктами владних повноважень та корпораціями в мережі. Наприклад, серед таких організацій слід назвати компанії, яка координуються суспільною організацію Access Now, яка відстежила зростання кількості відключень інтернету у світі [300].

У науковій літературі представлені позиції на розуміння поняття та природи цифрових прав. З погляду Т. Нортона, цифрові права є невід'ємними правами людини, що кожний публічний простір підлягає регулюванню так само, як і будь-яке право людини передбачає пошук певного балансу з іншими правами. Науковець звертає увагу на потребу максимального ефективного використання того, що пропонує цифрове середовище, яке дає змогу вільно й відкрито обмінюватися ідеями та водночас забезпечувати необхідний захист. Не ставити рівність між категоріями «неврегульований інтернет» та «вільний або відкритий інтернет» [691, с. 6]. До того ж, науковці висувають позицію, що намагання держав врегулювати інтернет може бути надмірними, створюючи перешкоди для здійснення цифрових прав [833, с. 4]. Відтак ідея цифрових прав привертає увагу та є темою для обговорення науковців.

У літературі висуваються різні позиції стосовно відношення цифрових прав до певних категорій та тлумачення як нової категорії прав людини. Перша група правників дотримується позиції щодо розуміння цифрових прав як самостійного нового напряму, як нової категорії XXI сторіччя, яке охоплює застосування публічно-правових та приватноправових конструкцій, не обмежуючись лише приватноправовими відносинами. Друга група правників дотримується думки на розуміння цифрових прав як похідних.

У «Посібнику із захисту цифрових прав та права вираження поглядів в інтернеті» зазначено, що категорія «цифрові права» охоплює права, які пов'язані з доступом до цифрових технологій та їх використанням, та вимагає розгляду кореспондуючих обов'язків з боку держави та інших суб'єктів, які гарантують, забезпечують здійснення та захисту цих прав [477].

Розглядаючи природу цифрової (електронної) особи як нової правової концепції Б. ван Бірз пропонує поширення прав людини, передбачених міжнародними Конвенціями та нормативно-правовими актами для визнання та захисту прав людини на його проєкцію – цифровий профіль в інтернеті [840, с. 559].

Означені права певною мірою повторюють зміст прав, які наразі називаються «цифровими». Аналогічні права О.Б. Братасюк, Н.Ф. Ментух відносять до цифрових прав: право на доступ до мережі «Інтернет»; право на свободу вираження поглядів – вільне висловлення своїх поглядів, пошук, отримання та поширення інформації онлайн; право на приватність та захист персональних даних; право на мирні зібрання, асоціації, використання електронних інструментів демократії – вільне об'єднання та використання сервісів для створення, приєднання, мобілізації та участі в соціальних групах та асоціаціях; право на свободу та особисту безпеку онлайн, здійснення якої потребує механізму захисту від протиправних дій, певних державних гарантій захисту від психологічного насильства чи домагань, мови нетерпимості та ворожнечі, недискримінації в інтернеті; право на цифрове самовизначення, право на відключення від онлайн або право бути забутим – особа вправі на власний розсуд визначити інформацію, яку буду використовувати в мережі[13, с. 58]. Аналогічний перелік цифрових прав пропонується Є. Гололобовою та А. Міна [36].

У межах даного дослідження увага приділяється приватноправовому аспекту цифрових прав.

Існують позиції, що цифрові права треба розглядати як об'єкти цивільних прав, що цифрові права є правами, які належать системам штучного інтелекту. Н.О. Тищук наголошує про доцільність законодавчої розробки категорії цифрових прав у контексті дослідження прав дитини, а саме: вчинення правочинів неповнолітніми та малолітніми особами в інтернеті, розуміє під цифровими правами дитини права майнового та немайнового характеру в мережі «Інтернет», які полягають у праві вільного доступу до мережі з урахуванням

медичних та психологічних рекомендацій та обмежень відповідно до віку; праві вільного висловлювання своїх думок у мережі; праві на інформацію; праві на приватність у мережі; праві на безпеку в мережі; праві вчинення правочинів з метою навчання, заробітку тощо [210, с.7]. М.В. Карандась висуває позиція про розгляд цифрових прав як групи особистих немайнових прав фізичних та юридичних осіб на вільний доступ, використання електронних пристрої та мереж комунікації [73, с. 173]. Розробники Концепції оновлення ЦК України наголошують на об'єктивації «цифрових прав» особи та потребу закріплення в законодавстві положень про «цифрові права» як різновиду особистих немайнових прав особи, що створюють можливість здійснення інтересів у сфері діджиталізації [82, с. 18]. Т.М. Ямненко, Д.О. Місько дотримуються позиції, що на сучасному етапі цифрові права людини є новою самостійною групою прав людини, що безпосередньо пов'язано з використанням цифрових технологій за допомогою додаткових електронних пристроїв та здійснюється в мережі «Інтернет»[285, с. 101]. Не виключаючи виділення нового комплексу цифрових прав та його потенції на внесення до четвертого покоління прав людини констатує О.М. Головко. Інформаційні та цифрові права співвідносяться як ціле і частина, що більшість цифрових прав є похідними від інформаційних та відображають сутність реалізації тих компетенцій, що має людина з високим рівнем інформаційної культури. Разом з цим науковець зазначає, що цифровізація, яка відбувається, призводить то формування наукового дискурсу, який спричиняє появу ідеї про виникнення нових прав: як право на використання віртуальної реальності, право на доступ до інтернету, право на доступ до цифрових знань та цифрової освіти тощо [35, с. 37].

Якщо розглядати цифрові права як нову концепцію прав, то постає питання про встановлення самостійних ознак, які б дозволили виокремити їх як відмінні або похідні від інших прав з урахуванням їх розподілу за поколіннями, галузевими властивостями, благами, які вони захищають, та ступенем їх універсальності [340; 514, с. 164]. За таких обставин постає питання співвідношення між цифровими правами і загальновизнаними правами з

урахуванням їх транскордонної технологічної специфіки, яка має в перспективі призвести до універсалізації правового режиму.

Тож у разі визнання концепції цифрових прав як нових прав, постає питання визнання проблематики розвитку законодавства, правозастосовчої практики та вирішення питання її співвідношення із існуючою правосуб'єктністю особи.

Крім того, наразі немає достатніх передумов для того, щоб віднести правовий статус суб'єктів у мережі «Інтернет» до будь-якої галузевої правової приналежності, оскільки діяльність суб'єктів у мережі пов'язана із здійсненням різних прав, таких як-то право на освіту, право на свободу слова та самовираження, право на свободу підприємницької діяльності, право на свободу мирних зібрань та свободу асоціацій, право на охорону здоров'я тощо.

До того ж слід зазначити, що з технологічною специфікою цифрового простору пов'язують природне походження окремих прав і свобод, наприклад, право на доступ до мережі «Інтернет», на захист персональних даних, право на анонімність, право на забуття, що дозволяє стверджувати про виникнення та розвиток прав нового покоління.

Проблематика означеного питання не завжди є очевидною, адже в Резолюції Генеральної Асамблеї ООН Право на приватність у цифрову добу від 18.12.2013 № A/RES/68/167 висловлений підхід, за яким права, якими людина володіє офлайн, мають захищатися в онлайн [820]. З урахуванням даного підходу, всі існуючі права, які юридично гарантуються та діють у реальному світі, за замовчуванням поширюються на віртуальне середовище. Щонайменше цим може обґрунтовуватися те, що категорія цифрові права служить меті узагальнення прав, які існують у фізичному середовищі, які також стосуються віртуальної реальності.

Надалі це правило було підтримане в Резолюції ООН про сприйняття, захист та здійснення прав людини в інтернеті від 27 червня 2016 року, яка прямо зазначає, що права передбачені Загальною декларацією прав людини та Міжнародним пактом про громадянські та політичні права особа має в інтернеті

та зауважує, що права, які особа має офлайн, мають також захищатися в мережі «Інтернет»; звертає увагу на право на свободу вираження поглядів у мережі «Інтернет» через зростаючу значущість інформаційних технологій [751].

Далі в Резолюції ООН Про заохочення та захист прав людини, громадянські, політичні, економічні, соціальні та культурні права, в тому числі право на розвиток від 18 червня 2018 повторюється дана теза.

Означена позиція підтримується Л. Опришко, який стверджує, що цифрові права, це ті ж права людини, гарантовані Конституцією України [78] та Конвенцією про захист прав людини, але які реалізовуються в цифровому середовищі [87].

Аналогічну позицію відстоюють Н. Лесько, М. Антонов, що для розуміння прав людини в онлайн-середовищі використовується поняття цифрові права, як норми та правила поведінки, які закріплюють права та свободи людини щодо належного доступу та використання електронних пристроїв, створення та використання цифрових творів[97, с. 160].

Непоодиноко висуваються тези про цифрові права як умовну категорію, що охоплює особливості здійснення та захисту фундаментальних прав людини в інтернеті, зокрема свободи вираження поглядів та права на приватність онлайн тощо, а не окремої групи прав людини [137, с. 6].

Відтак В. Володовська дотримується погляду щодо цифрових прав як умовної категорії, яка визначає особливості здійснення та гарантії захисту прав людини в інтернеті. З огляду на істотну роль, яку відіграє інтернет, авторка пропонує так би мовити уявити «Декларацію цифрових прав людини», в якій об’єднати всі правові можливості людини в онлайн- середовищі та обов’язки влади щодо їх реалізації [25].

Підтримує дану позицію М.Г. Хаустова та зазначає, що покоління прав людини еволюціонують разом із розвитком цифрових технологій, а сфера дії раніше існуючих прав розширюється, з’являються нові права [266, с. 330].

З урахуванням означеного, на погляд Ю.С. Размєтаєвої, категорія «цифрові права людини» охоплює два розуміння. У першому розумінні, під ними

називають усі ті права, здійснення та захист яких тісно пов’язаний сьогодні з використанням цифрових інструментів або має суттєву онлайн-складову. У другому – лише ті права, які виникають або починають претендувати на статус фундаментальних в умовах цифрових трансформацій. Тому до цифрових відносять такі фундаментальні права як свобода вираження думки і слова, недоторканність приватного життя, право на інформацію, право на участь в управлінні державними справами тощо, і такі як право бути забутим, право на анонімність та право на інтернет [174, с. 18].

І.Е. Ревуцька дотримується позиції, що віртуальні права включають широкий спектр прав, які реалізовуються із використанням цифрового середовища та потребують врахування властивостей цього середовища [136, с. 212].

Г. Гогін, А. Вромен, К. Везеролл у дослідженні, присвяченому цифровим правам в Австралії застосовують широкий, плюралістичний підхід до розуміння цифрових прав, який охоплює: права, чітко викладені або визнані в нормативно-правових актах; ідеях та практиках прав людини, розроблених організаціями та окремими особами; права, які виходять за традиційні межі держав, національних, регіональних та міжнародних спільнот держав [540, с. 18]. З огляду на мету дослідження, австралійські правники фокусують свою увагу на таких сферах розвитку цифрових прав як приватність, профілювання та аналітика; порівняння даних, які обробляють державні органи, та спостереження; трудові відносини; вираження свободи слова, зазначаючи зокрема про розвиток цифрових прав в галузі інтелектуальної власності, цифровому урядуванні та цифрове громадянство тощо.

У своєму дослідженні К. Карпінена та О. Пюко розглядають цифрові права в межах чотирьох концепцій: цифрові права як захист негативних свобод; цифрові права як позитивні права та обов’язки держави; цифрові права як засіб інформаційної справедливості; цифрові права як можливості, які надаються онлайн-платформами [594, с. 304].

Дискурс про концепцію цифрових прав як засобу захисту негативних свобод окремих осіб або корпорацій, які переслідують свої інтереси, виражається у вільних від державного втручання та регулювання гарантій правових норм та обмежень державної влади. Попри те, що розгляд цифрових прав як негативних прав та свобод значний час був досить поширеним, наразі більшість громадських організацій (які були прибічниками вільного інтернету) визнають потребу виваженого підходу у правому регулюванні цифрового середовища та забезпечення захисту здійснення цифрових прав у мережі.

Відповідно до концепції цифрових прав як позитивних прав та обов'язків держави, здійснення прав особи в інтернеті розглядається як обов'язок держави на національному та наднаціональному рівні забезпечити здійснення прав, серед яких рівний доступ до мережі «Інтернет». Так, замість невтручання в регулювання, за даною позицією, висувається ідея створення нормативних та інституційних механізмів для здійснення та захисту прав у мережі «Інтернет». Наприклад, свобода вираження думки, права людини другого та третього покоління, такі як право на розвиток та право на участь у повсякденному житті, пов'язані з рівними умовами та можливостями використання цифрових інструментів, а саме – доступу до мережі. У межах даної позиції цифрові ЗМІ розглядають цифрові права як інфраструктури для здійснення та заохочення прав людини в цілому. Як зазначається в доповіді РНБ ООН за 2011 рік, через трансформаційний характер цифрових технологій доступ до цих технологій та здатність ефективно їх використовувати слід розглядати як незамінний інструмент для здійснення цілої низки прав людини. З погляду К. Матієсена, доступ до інтернету можна розглядати як похідне право людини, яке випливає із основоположних прав людини, здійснення яких здебільшого залежить від доступу до інтернету та цифрових технологій [655, с. 3].

Дотримуються концепції цифрових прав як позитивних прав суб'єкти владних повноважень, як наприклад, Шведська агенція з міжнародного розвитку (SIDA), яка у 2019 році виразила занепокоєння зменшенням вільного,

демократичного простору в інтернеті, оскільки саме відкрите цифрове середовище є рушійною силою розвитку суспільства та інновацій [655, с. 3].

Поряд із такими державами як КНР, яка вживає заходи для контролювання інформаційних потоків та суворого регулювання інтернету, превалюють ліберальні підходи правового регулювання вільного інтернету, заснованого на забезпечені здійснення основних прав свобод людини [767, с. 310]. На регіональному рівні дана концепція цифрових прав простежується в таких актах як Хартія фундаментальних цифрових прав Європейського Союзу, метою якої є побудова та розширення існуючих фундаментальних прав та обов'язків ЄС[424].

Концепція цифрових прав як засобу інформаційної справедливості приділяє увагу забезпеченню цифрових прав не лише окремих осіб та організацій, а й захисту прав вразливих груп та проблемі концентрація влади в обмеженого кола осіб. Дана концепція певною мірою близька до концепції цифрових прав як позитивних, та приділяє увагу забезпеченню рівного доступу та наділення рівними правами осіб. Водночас, за даним підходом, цифрові права розглядаються більш широко як засіб забезпечення інформаційної справедливості та доступу до інформаційних ресурсів[594, с. 305].

Крім очевидного впливу на свободу вираження поглядів особи, дана концепція розглядає цифрові ЗМІ як інструмент, який дозволяє просувати цифрові права як елемент економічного розвитку, політичної участі, боротьби з нерівністю та розвитком суспільства у віртуальному середовищі загалом.

Відтак концепцію цифрових прав як елемента інформаційної справедливості об'єднують такі аспекти як цифрова нерівність, цифровий розрив, контролювання та домінування в інтернеті тощо. Дана концепція зосереджена на дихотомії прав людини та домінуванні компаній. Серед загроз цифровим правам, які несуть цифрові Інтернет-гіганти, називається комерціалізація комунікації, створення олігополій, монополізація доступу до контенту, зловживання автономними системам, які можуть поглиблювати соціальну та культурну нерівність в інтернеті.

Елементи концепції можна простежити в діяльності правозахисних та неурядових організацій, які приділяють увагу аспектам соціальної справедливості, цифрової нерівності, демократичному розвитку та регулюванню вільного інтернету. З погляду М. Фетчеріна, вперше концепція цифрових прав як така була представлена саме інтернет-спільнотами, європейськими правозахисними організаціями, які здійснюють діяльність із захисту фундаментальних прав та свобод людини в цифровому просторі, приймають акти рекомендаційного характеру [514, с. 165].

Відповідно до думки К. Карпінена та О. Пюко, концепція цифрових прав як можливостей, що надаються онлайн-платформами, охоплює роль держави та наднаціональних організацій як соціальних регуляторів у забезпечені та здійсненні цифрових прав. Цифрові права розглядаються як права, що надаються GAFA. Цифрові права можуть бути визначені як вчинки або дії, які уповноважує вчиняти технологія завдяки своєму дизайну [594, с. 305]. Тож цифрові права розглядаються не як надані та забезпечені державною, а як вбудована частина цифрової архітектури. У певному сенсі відповідно до даної концепції, GAFA отримує статус регулятора правовідносин та нормотворця в мережі.

У межах даної концепції актуальною є заява М. Цукерберга про створення наглядової ради за контентом на платформі, під назвою Верховного суду Facebook. Передбачається, що до її складу мають увійти провідні правники та фахівці США [88; 260]. Означене свідчить про прагнення корпорації набути більшого контролю за управлінням та поширенням контенту в мережі.

Дискусії, що «код є законом», «мережева архітектура є політикою», здатності програмного коду замінити закон як регулятора відносин у мережі, неминуче актуалізує проблему здійснення прав людини, таких як право на вираження, недоторканності приватного життя, виникаючі ризики дискримінації та нерівності. Значну увагу про зростаючу роль інтернету та «програмного коду як закону нової якості» приділяє Л. Лессіг [636, с. 50]. Є.О Харитонов та О.І. Харитонова зазначають, що регулювання в інтернеті може здійснюватися двома

шляхами: за допомогою правового регулювання та за допомогою ІТ-засобів, а саме програмного коду [68, с. 83].

На думку С. Хасан та П. Філіппі, на відміну від правового регулювання, яке передбачає межі дозволеної поведінки, технічні або програмні норми від початку визначають допустиму поведінку, що усуває необхідність застосування інших засобів впливу та норми права. Програмний код переважно визначає межі дозволеної поведінки в мережі, що може бути більш ефективним з огляду на специфіку архітектури інтернету, та відсутності необхідності покладатися на здійснення нагляду за дотриманням законодавства на третіх осіб (правоохоронні органи) [522; 550, с. 88].

Б. Розенблат наводить як приклад регулювання комп'ютерним кодом, управління цифровими правами (DRM), які імплементують закон про авторське право на технологічні засоби захисту, обмежуючи використання, розпорядження та копіювання творами, захищеними авторським правом [775, с. 288].

Про активне поширення програмного коду як регулятора цивільних відносин у мережі «Інтернет» свідчить застосування смарт-контрактів, які являють собою програмний код (який зберігається в децентралізованій системі блокчейн), який містить умови договору, призначені для автоматичного дотримання та виконання сторонами, без необхідності залучення посередників [99, с. 39; 456, с. 544]. Застосування технології блокчейн та програмного коду покликано автоматизувати виконання договірних конструкцій, оптимізували прийняття рішень у сфері державного управління, судочинства та виконання судових рішень [457, с. 3].

Урядами держав поступово проваджується використання автоматичних алгоритмів у державному управлінні. Наприклад, уряд США включив перелік осіб, яким обмежений доступ користування авіаційним транспортом та участь у польотах до алгоритму прогнозування загроз національної безпеки [431, с. 1249]. Алгоритм використовується зокрема на досудовому розслідуванні, виявлені зловживання користування субсидіями. В Україні використання за допомогою

коду застосовується в додатку «Дія» під час надання доступу до державних послуг, при нарахуванні виплат тимчасово переміщеним особам тощо.

К. Оніл припускає, що способом подолати суб'єктивізм, зокрема під час найму на роботу, може стати усунення людини від процесу прийняття рішень, а прийняття рішень за допомогою коду [698, с. 287]. Визнаючи використання програмного коду як засобу регулювання цивільних відносини в інтернеті, слід брати до уваги, що регулювання за допомогою коду приховує в собі недоліки, оскільки алгоритми посилюють дію неупередженостей та врешті посилюють суб'єктивізм, якого прагнуть позбутися. Тож визначаючи розуміння цифрових прав як нового етапу прав людини, які обумовлені існуванням мережі та інформаційно-комунікаційних технологій, не можливо оминути специфіку архітектури інтернету та застосування програмного коду для визначення меж дозволеної поведінки в мережі.

Програмний код може створюватися приватними та державними платформами. Будучи частиною державної інформаційної системи, створений та санкціонований, програмний код, фактично набуває сили закону. Означене актуалізує питання, чи займе програмний код в майбутньому своє місце поряд з іншими регуляторами суспільних відносин, безпосередньо або опосередковано взаємодіючими між собою (правом та мораль), чи навпаки, займе місце форми (джерела) прав на умовах взаємодії з іншими формами, а саме нормативно-правовими актами. Ми дотримуємося позиції, що програмний код у системах органів державної влади та місцевого самоврядування може містити вимоги до поведінки суб'єктів відносин у мережі «Інтернет», безпосередньо впливати на права та обов'язки, та шляхи їх реалізації. Поряд із цим, програмний код може не відповідати змісту нормативно-правових актів та приписів закону. Тому актуальним є забезпечення пріоритетності положень законів та нормативно-правових актів над правилами, вимогами та обмеженнями, які впроваджує програмний код.

У мережі особливої ролі набувають умови користування платформами, які розробляються приватними компаніями. З погляду А. Калламарда, концепція

наділення компаній правомочностями в управлінні цифровими правами [360, с. 192] відображена в Керівних принципів ООН у сфері бізнесу та прав людини або «принципах Раггі», які вимагають від компанії в інтернеті: обов'язку захищати права людини від порушень; корпоративну відповідальність за дотримання прав людини; доступ до засобів захисту жертв зловживань, пов'язаних із бізнесом [822]. На думку науковця, три стовпи цієї концепції стверджують, що обов'язок держави захищати від порушень прав людини поширюється і на бізнес, компанії повинні уникати порушень прав і усувати негативні наслідки, а жертви повинні мати доступ до засобів правового захисту.

На основі цих принципів складається Індекс рейтингу цифрових прав, який визначає світових лідерів у сфері інформаційно-комунікаційних технологій за обсягом зобов'язань, політикою, впливом на свободу вираження поглядів та приватності користувачів. Основною метою Рейтингу є не вплив на регулювання та забезпечення дотримання законних прав компаніями, а не лише допомога компаніям покращити умови користувацьких угод, а підвищити обізнаність користувачів [760].

Слід зазначити, що науковці приділяють увагу нагальній потребі щодо прав людини, які слід розглядати не як корпоративні обов'язки та додаткову відповідальність компаній, а як основоположні права, яких дотримуються корпорації.

Поряд із викладеними концепціями існують твердження науковців, які ставлять під сумнів концепцію цифрових прав з позиції їх економічної сили. Й. Ріке та М. Марзукі стверджують, що корпоративне підґрунтя та оформлення прав людини в мережі «Інтернет» може призвести до переходу від «правового регулювання» до «корпоративної соціальної відповідальності», що загрожуватиме ефективному захисту всіх прав людини [772, с. 3].

Правове становище користувачів, окрім законодавчо закріплених прав, обов'язків та відповідальності в межах певної юрисдикції, регулюється правами та обов'язками, взятими на себе суб'єктом за договором із цифровою платформою (соціальними мережами, ігровими платформами тощо), які

становлять основу функціонування інтернету загалом, і використання ресурсів глобальної мережі зокрема.

При цьому правовий статус фізичних осіб, сформований на підставі законодавчо закріплених прав та обов'язків, передбачених у нормативних правових актах різного галузевого спрямування, має братися до уваги під час коригування правового регулювання відносин в умовах розвитку правових відносин у мережі «Інтернет».

Поряд із тлумаченням «цифрових прав» у науці проводяться дискусії щодо прав учасників віртуальних світів. Так Р. Костер, який розробив на підставі Декларації прав людини Декларацію прав аватарів у 2000 році, для встановлення та нагадування «мешканцям» віртуальних світів усіх видів, які володіють владою над віртуальним простором про їх права та обов’язки, який під «аватаром» розуміє втілення реальної особи в онлайн-просторі, а його висловлювання, дії, думки та емоції слід вважати такими ж чинними, як висловлювання, дії, думки та емоції людей у будь-якому іншому форумі, місці проведення або просторі. У Декларації аватари розглядаються як людина, наділена тими ж свободами. На переконання науковця, найважливішим з цих прав є право, щоб з аватаром поводилися як з людиною, а не як безтілесною, безглуздою, бездушною маріонеткою, а права аватара безпосередньо пов’язані із обов’язками адміністратора, та складно притягнути адміністратора за вчинки гравців [603].

Е. Кастронова у своїй роботі 2003 року передбачає такі права цифрової особи: вільне пересування та об’єднання (особа має право вільно залишати віртуальні світи та входити до них за бажанням, вільно формувати спільноти; бути вільною від переслідування в мережі); вільне отримання інформації (право вільної кореспонденції та отримання інформації із різних джерел, в том числі за межами віртуального середовища); вільне вираження (свобода вираження та творчості, участі в політичному житті, формуванні політичної повістки, розробка коду, який має підпорядковуватися волі людей). Більшість даних прав гарантовані в державах, а з тим додаткове приділення уваги закріпленню цих

прав мало б бути зайвим, водночас, як свідчить практика, у віртуальних світах має місце порушення даних прав [419, с. 37].

Т. Дей звертає увагу, що права аватарів безпосередньо пов'язані з обов'язками адміністраторів, яких подекуди складно притягнути до відповідальності за вчинки гравців[453, с. 137]. На обсяг прав та обов'язків фізичної особи в мережі «Інтернет» може впливати статус суб'єкта в певній соціальній спільноті, який може формалізуватися за допомогою процедур, мати юридично та технічно визначений та забезпечений характер, як-то модератор форуму, сторінки, групи тощо. Водночас коло прав та обов'язків може носити також неформальний характер, будучи не підкріпленими певними повноваженнями особи в мережі. Разом з тим цифрова репутація як інструмент соціального впливу, здатна привернути до користувача значне коло підписників, зібрати спільноту навколо його цінностей та ідей.

На думку Б. Дюранске, правила ігор виступають регулятором відносин у мережі. Користувацькі правила ігор та платформ можуть містити положення про відшкодування шкоди, накладення покарання та принципи самозахисту, передбачені нормами кримінального та адміністративного права [488, с. 50]. Користувацькі угоди ігор, таких як Second Life містить правила поведінки та стандарти спільноти, які не допускають вираження нетерпимості, переслідування, розголошення інформації, та санкції за порушення правил віртуального середовища, в тому числі підстави тимчасового призупинення та припинення дії облікового запису [813].

З погляду С. Кроуфорда, саме поняття «права» передбачає вже існування низки уявлень, що захищають особу від ієрархії, і не відповідає динамічному, контекстуальному світу ідентичності. З цієї причини наявність якогось централізованого універсального «закону ідентичності» (і пов'язаних із нею прав) не мають сенсу: оскільки не постає повністю сформований контекст ідентичностей, а різні групи мають різні способи розв'язання питань із видалення ідентичності. Марно (і, можливо, руйнівно) припускати, що люди можуть заздалегідь розробити правила та умови видалення ідентичності, яких

мають дотримуватися віртуальні світи[445, с. 8]. Аналіз думок науковців, дозволяє стверджувати, що під «ідентичністю» науковці переважно розуміють цифровий акаунт фізичної особи, створений у певній інформаційно-комунікаційній системі, або цифрову ідентичність у вузькому розумінні.

У такий спосіб, слід констатувати, що попри поширене використання терміна «цифрові права», єдність розуміння його змісту відсутня, та переважно зводиться до розуміння як універсальних прав людини, адаптованих до умов інформаційного суспільства, здійснення та захист яких пов'язані із використанням інформаційно-комунікаційних технологій, зокрема права на недоторканність приватного життя, право на доступ до мережі, створення та використання цифрових об'єктів тощо. У такому розумінні фактично синонімами терміна «цифрові права» використовуються такі категорії як «віртуальні права», «комунікаційні права», «інформаційні права» без проведення чіткого розмежування між цими категоріями.

Якщо перекладати digital law та digital rights, то law позначає закон або право в об'єктивному розумінні, а rights – права в більш вузькому розумінні. Відтак у літературі цифрове право, digital law використовується переважно в розумінні сукупності правових норм, різних галузей права, які стосуються відносин, що виникають у мережі «Інтернет», таке розуміння є синонімічним інформаційному праву або інтернет-праву. Цифрові права або digital rights є суб'єктивними правами, не природними правами, які походять від природи людини як біологічного виду.

З огляду на розглянуті погляди, ми вважаємо, що цифрові права слід розуміти як новий етап розвитку прав людини, який обумовлений функціонуванням інтернету та інформаційно-комунікаційними технологіями (право вільного доступу до мережі; право на інформацію та доступ до інтернету; право на приватність у мережі; право на безпеку в мережі; та інші права) в тому числі традиційних прав, здійснення яких відбувається в мережі та здійснення яких забезпечується за допомогою норм правового регулювання, та за допомогою застосування програмного коду.

Р.О. Стефанчук по відношенню до особистих немайнових прав у сфері сімейних відносин звертає увагу, що опосередкування певної правової можливості поняттям «суб'єктивне цивільне право» означає, що вона забезпечує його юридичним обов'язком дотримання та не порушення права, а невиконання обов'язку призведе до настання правових наслідків у вигляді юридичної відповідальності [203, с.108]. Інакше такі права будуть носити лише декларативний характер.

На наш погляд, поряд із переосмисленням багатьох правових конструкцій через розвиток інтернету, права, які виникають у цифровому середовищі, будучи правами людини, лише змінили форму свого існування, а не зміст. Тому солідаризуємося з позиціями науковців, які розглядають цифрові права та обов'язки як наступний етап еволюції прав людини, адже трансформаційних змін зазнають особисті немайнові та майнові права та обов'язки.

Відтак цифрове право в суб'єктивному значенні є визначеною нормами права, забезпечена актами саморегулювання міра можливої поведінки особи, що гарантує їй вільний вибір, яка визначається правовою нормою. У такому сенсі – це частина змісту загальної правоздатності, яка буде постійно удосконалюватися на наповнюватися новими правомочностями, інакше логічно висунути концепт цифроздатності як різновиду правоздатності на кшалт сімейної, активної тестаментоздатності.

Тож правосуб'єктність фізичної особи в мережі «Інтернет» складають цифрові права, які можна визначити як різновид прав людини нового покоління, що виражені в цифровому середовищі, обумовлені функціонуванням інтернету та інформаційно-комунікаційними технологіями, в тому числі традиційних прав, здійснення яких відбувається в мережі, здійснення та дотримання яких забезпечується за допомогою правових засобів та за допомогою застосування програмного коду (архітектури інформаційної системи) автоматично. Цифрові права не є природними правами, які походять від природи людини як біологічного виду. До цифрових прав можна віднести особисті немайнові та майнові права, здійснення яких обумовлено існуванням мережі та інформаційно-

комунікаційних систем (право вільного доступу до мережі; право на інформацію та доступ до інтернету; право на приватність; право на безпеку; право на доступ до даних; право не піддаватися рішенню, заснованому виключно на автоматизованій обробці персональних даних; право на роз'яснення індивідуального рішення, прийнятого за допомогою автоматизованих систем; право на забуття; право на виправлення неточних даних та результати профілювання; право на перенесення даних; право на обмеження обробки даних) та традиційні права, здійснення яких відбувається в мережі.

Підсумовуючи викладене, слід зазначити, що використання технологій несе за своєю суттю накопичувальний ефект, який може відображатися в поєднані (симбіозі) права та технологій, у результаті чого останні починають відігравати роль правових інструментів у різних сферах. Поряд із позитивним ефектом від використання технологій, така ситуація може призводити до ризиків порушення та нівелювання прав суб'єктів.

Наразі технології не набули ознак самостійності, вбудовуються в існуючу правову систему, доповнюючи та розширюючи її. З урахуванням таких трансформацій, перед юриспруденцією постає задача ефективної розробки та накопичення досвіду взаємодії юридичних та техніко-алгоритмічних засобів. Для недопущення виникнення змагальності або конфліктів між правовими засобами регулювання та технологіями (програмним кодом), необхідно дотримання принципу пріоритетності правових інструментів, підходів та методів, та вживання заходів, які не допускають повне заміщення правових засобів регулювання на технології. Означене особливо актуалізується у випаду виникнення ізольованих середовищ в інтернеті (метасвітів).

3.3. Особисті немайнові права у складі цивільної правоздатності фізичної особи в мережі «Інтернет».

3.3.1. Право на недоторканність приватного життя в мережі «Інтернет»

Бурхливий розвиток технологій та зростання кількості об'єктів, підключених до мережі «Інтернет», посилює ризики втручання в недоторканність приватного життя. Системи та речі, будучи підключеними до мережі, збирають персональні дані, які стали «новою нафтою», ресурсом для розвитку сервісів платформ та автоматизованих систем. З одного боку, великі обсяги збору та обробки персональних даних викликають у користувачів побоювання порушення приватності [606, с. 430], з іншого боку, невідворотно впливають на здійснення прав та обов'язків у такому, майже квазі фізичному світі.

Аналіз персональних даних використовується приватними, державними організаціями для: оцінки кредитоспроможності клієнтів; покращення послуг; виявлення шахрайства, зловживань правами та іншої злочинної діяльності; проведення досліджень тощо. Прикладом надмірного збору персональних даних, що створює загрозу втручання у приватність, є пошукові системи Google. За твердженням Г. Шасло, колишнього інженера Google, проблема полягає в тому, що користувачі надають Google набагато більше даних, ніж необхідно, у свою чергу, Google зберігає дані надмірно довгий час ніж це потрібно для цілей обробки [686].

Глобальний характер інтернету та бурхливий розвиток інформаційно-комунікаційних технологій називається в Резолюції Генеральної Асамблеї ООН від 18.12.2013 № 68/167 «Право на недоторканність особистого життя в цифрову добу», однією із рушійних сил прискорення прогресу на шляху його розвитку в різних формах [820]. У Резолюції підтверджується, що право на особисте життя не повинно зазнавати дозвільного або незаконного втручання в недоторканність житла або таємницю кореспонденції, та право на захист від такого втручання, як це передбачено у ст. 12 ЗДПЛ та ст. 17 МПГПП. У Резолюції наголошується

потреба захисту прав, якими людина володіє в офлайн-середовищі, включаючи право на недоторканість особистого життя. Що всі держави зобов'язані поважати та захищати право на недоторканність приватного життя, в тому числі в контексті цифрової комунікації, а також запобігати порушенню таких прав.

У доповіді Ради Європи щодо верховенства права в інтернеті та цифровому світі 2014 року зазначено, що цифрове середовище може завдяки своїй природі розмивати засади приватного життя та фундаментальних прав, підриваючи відповідальне прийняття рішень. Що криється потенційна вірогідність підриву верховенства права шляхом послаблення права на приватне життя тощо [821]. Проте, як випливає з даної доповіді, обмеження доступу до мережі та цифрових ЗМІ, спроби моніторингу онлайн-діяльності та електронних комунікацій є втручанням у свободу вираження думки, свободу об'єднань, особисте та приватне життя (також втручання в такі права як свобода совісті та віросповідання, права на справедливий судовий розгляд).

Право на недоторканність приватного життя визначає межі автономії фізичної особи в сучасному суспільстві, у свою чергу, така сфера приватного життя має бути вільна від втручання державної влади (проявляється негативний обов'язок держави) та поряд із цим державні органи мають вживати заходи, щоб захищати приватне життя від втручання приватних суб'єктів (прояв позитивного обов'язку держави).

Стосовно українського законодавства, то забезпечення права на недоторканність приватного життя кожної людини в Україні відповідно до міжнародних, у тому числі європейських, стандартів зазначено як стратегічну ціль згідно з пар. 6 Указу Президента України Про Національну стратегію у сфері прав людини від 24 березня 2021 року №119/2021, для чого вимагається вирішення проблеми неузгодженості законодавства України про захист персональних даних з європейськими стандартами [160].

У вітчизняній доктрині переважно використовується категорія «недоторканність приватного життя», поряд із якою наразі отримало поширення застосування поняття «приватність» або «privacy» в роботах Р.В. Романова [185,

с. 6], О.М. Калітенко [70, с. 51], Н.С. Марценко[103, с. 223], Р.О. Стефанчука [204, с. 476], С. Булавіної, Т. Давидової [17, с. 8], В.А. Сокуренко, Н.О. Хрякової [198, с. 280] тощо. В Оксфордському юридичному словнику «privacy» позначає право «бути залишеним у спокої». «Privacy» визначається як право на приватне життя відповідно до змісту передбаченого у ст. 8 ЄКПЛ «Право на повагу до приватного та сімейного життя» [731, с. 410].

Тож слід погодитися з О.В. Горпинюк, що застосування слова «приватність» в українській термінології є наслідком перекладу англійського терміна «privacy», який вживається в англомовній літературі [46, с. 18]. На думку П.Д. Гуйвана, право на приватність включає недоторканність особистої інформації про інтимні, особисті сторони свого приватного буття [48, с. 179]. З огляду на те, що зміст даної категорії варіюється залежно від юрисдикції, з урахуванням того, що Україна орієнтується і традиційно підтримує цінності та ідеї західного суспільства, логічним є звернення до інтерпретації поняття «приватність» або недоторканність приватного життя, яке розробляється в західній доктрині та судовій практиці.

Традиційно вважається, що вперше визначення приватності було сформульовано С. Уорреном та суддею США Л. Брандейсом у 1890 році як «права бути залишеними у спокої» [853, с. 194]. Водночас за твердженням Дж. Блекмана, від початку концепція недоторканність приватного життя зародилася в доктрині США та була висунута Т. Кулі, а відомою стала вже завдяки публікації С. Уоррена та Л. Брандейса [339, с. 362].

Поштовхом для формулювання визначення приватності вважається винайдення фотокамер Eastman Kodak наприкінці XIX ст., яке поставило питання кваліфікації дій фотографів, які використовували камери та робили фото не отримавши згоду фізичної особи [673, с. 25].

Формулюючи межі приватності С. Уоррен та суддя Л. Брандейс визначили, що право на приватність не поширюється на осіб, «які відмовилися від права жити власним життям, прихованим від публічного спостереження», маючи на

увазі кандидатів на державні посади та осіб, які займають державні посади та займаються публічною діяльністю.

Значний вплив на розвиток концепції приватності здійснила справа Gill v. HearstPublishing[383], де Суддя Картер проводячи відмінність між публічними особами та особами, які бажають «залишитися у спокої», довів необхідність поваги до приватного життя непублічних осіб та визнання публічного поширення фактів приватного життя відносно таких осіб порушенням їх прав.

Дана позиція знайшла своє відображення в положеннях Декларації про свободу політичних дебатів у засобах масової інформації, схваленої 12.02.2004 року на 872-му засіданні Комітету Міністрів Ради Європи [466] та рекомендації Резолюції № 1165 (1998) ПАРЄ Право на приватність [139]. Відповідно до норм декларації, коли особа погоджується стати державним службовцем, публічним діячем, вона за замовченням має усвідомлювати, що може бути піддана гострій критиці з боку суспільства, а межа можливої критики публічної особи є значно ширшою, аніж непублічного громадянина. Аналогічно Конституційний Суд України зазначив, що втручання в особисте та сімейне життя особи, яка обіймає посаду, пов'язану із виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень допускається винятково у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [176]. Дане положення повністю обґрунтовується публічним інтересом до діяльності таких осіб [52, с. 131].

Чинне законодавство ЄС та Закон України «Про захист персональних даних» надає суб'єктам низку прав, які дозволяють їм приймати юридично значущі рішення стосовно недоторканності власного приватного життя. За твердженням П.М. Шварца, провідними засадами правового регулювання приватності є принцип поінформованості суб'єктів про обробку та право надання згоди на обробку персональних даних [783, с. 1966].

К. Кумаяма стверджує, що розуміння приватності пов'язано із ідентичністю та свободою особи, розрізняючи в межах категорії дві складові:

«інформаційну приватність» та «приватність при прийнятті рішень». Інформаційна приватність – це право особи обмежувати та контролювати «здатність інших осіб отримувати, поширювати, використовувати інформацію про нього». Приватність при прийнятті рішень включає право особи приймати рішення стосовно свого приватного життя, сім'ї, дітей, особистих відносин тощо [771, с. 1087]. Дані аспекти перетинаються, водночас судова практика США передбачає переважний захист саме здійснення права на приватність при прийнятті рішень, визнаючи його фундаментальним правом [797, с. 250].

В інтернеті гостро стоїть проблема втручання у сферу прийняття рішень користувачів через постійний вплив персоніфікованих новин та таргетованої реклами, маніпуляції користувачів до вчинення певних дій (придбання товарів, послуг, голосування за певного кандидата тощо) [882, с. 210].

Закріплення права на недоторканність приватного життя отримало своє поширення в конституціях держав континентальної правової системи, які були прийняті після Другої світової війни. Так, ФРН характеризується сталою традицією захисту недоторканності приватного життя та верховенства права. У 1983 р. Федеральний Конституційний суд ФРН ухвалив рішення, яким визнав право на вільний розвиток особи та право на інформаційне самовизначення (можливість встановлювати форми використання даних про особу)[354].

На погляд Е. Фіалова, таке визначення є близьким до визначення приватності як права особи на власний розсуд визначати, коли та в якій мірі персональні дані про них передаються іншим особам [521, с. 47]. Т. Хохімстра визначає право на інформаційне самовизначення як право особи визначати межі, використання і поширення особистої інформації з метою самовизначення[565, с. 162]. А. Флюкігер, зазначає, що право на самовизначення у сфері персональних даних гарантує кожному право приймати рішення щодо поширення та використання його персональних даних [518, с. 837].

О.Б. Братасюк, Н.Ф. Ментух виражають позицію, що під правом на цифрове самовизначення розуміється не лише право на власний розсуд

визначати інформацію про особу, яку вона буде використовувати в системі, а й право на відключення від онлайну або право бути забутим в інтернеті [13, с. 60].

На погляд Дж. Рейденберга, такий підхід європейського законодавця допомагає прояснити різницю у підходах до правового регулювання недоторканності приватного життя та захисту персональних даних в ЄС та США [766, с. 1330].

Слід констатувати, що право на недоторканність приватного життя перетинається із правом на захист персональних даних, разом з цим у доктрині висуваються різні підходи до питання співвідношення недоторканності приватного життя та персональних даних.

Відповідно до Інструкції Європейського дорадчого органу із захисту персональних даних та приватності 4/2007 «Щодо концепції персональних даних»[708], правила захисту персональних даних виходять за межі широкого поняття права на повагу приватного та сімейного життя. Доцільно зазначити, що Хартія ЄС про основні права закріплює захист персональних даних у ст. 8 як автономне право, поряд із правом на приватне життя, передбачене у ст. 7, відповідно Регламент ЄС 2016/679 та Директива 95/46 ЄС мітять застереження, що їх сфера застосування поширюється на випадки обробки персональних даних за межами дому та сім'ї, якщо обробка передбачена трудовим законодавством, необхідна для цілей судочинства або для прямого маркетингу та ін. Означений підхід виходить з того, що захист персональних даних поширюється на різні сфери не лише приватного життя людини, з тим персональні дані є значно ширшою категорією та виходять за межі приватного життя.

Завдяки практиці застосування ст. 8 ЄКПЛ[77], розуміння категорії недоторканність приватного життя у практиці ЄСПЛ є досить широкою категорією та за містом виходить за межі особистого, сімейного життя [90, с. 105; 50, с. 101]. Рішення ЄСПЛ не передбачають єдиного та вичерпного тлумачення поняття приватне життя. Питання збору, обробки, здійснення права на доступ персональних даних розглядається як складова категорія недоторканність приватного життя (Leander v. Sweden, 1987) [392], поряд із правом на доступ до

даних про родинні зв’язки та спростування таких зв’язків (Graham Gaskin v. the United Kingdom, 1983 [384], встановленням та спростуванням батьківства (Rasmussen v. Denmark, 1984) [405] недоторканістю приватних приміщень та професійної кореспонденції (Niemietz v. Germany, 1992) [398], можливістю публікації фотографій особистого характеру (Von Hannover v. Germany, 2012) [415] та свободою вираження журналістів в оприлюдненні подій, які мають суспільний інтерес та стосуються публічних осіб (Axel Springer AG v. Germany, 2012) [367].

Дана позиція підтримується у роботах вітчизняних науковців Т.В. Бачинського, Р.І. Радейко, О.І. Харитонова[123, с. 50], П.Д. Гуйвана [49, с. 110; 50, с. 101].

Недоторканність персональних даних фізичної особи пов’язують із таким різновидом недоторканності приватного життя як інформаційна приватність.

Право на самостійне визначення режиму доступу до відомостей персонального характеру (в тому числі залишення їх в таємниці), право на ознайомлення з даними про себе в органах публічної влади та внесення змін до відповідних баз даних, В. Серьогін називає правом на інформаційну приватність. На погляд науковця, розуміння такої категорії як недоторканність дає змогу більш чітко з’ясувати зміст та обсяг права на недоторканність приватного життя. Недоторканність відносно інформаційної приватності позначає неприпустимість будь-якої інформаційної діяльності (збору, зберігання, поширення та використання) стосовно персональних даних без згоди особи, відносно якої воно стосується [194, с. 89].

На погляд К.І. Пономаренка, під інформаційною приватністю на сучасному рівні розвитку суспільства доцільно розуміти такий стан фізичної особи, за якого вона як носій та першоджерело інформації про себе має виключне право нею розпоряджатися, розголошувати, приховувати, передавати або змінювати цю інформацію [172, с. 115].

У науці також існує позиція про уточнення поняття інформаційної приватності за допомогою застування терміна «недоторканність цифрової та телекомунікаційної сфери приватного життя».

Громадська організація «Приватність та права людини» називає поряд із фізичною, територіальною та майновою приватністю, інформаційну приватність та приватність комунікації [746]. Така класифікація недоторканності приватного життя набула розвитку та була розкрита у подальших дослідженнях: Т.О. Софіюк [197, с. 255], О.М. Калітенко [70, с. 52], Дж. Холвастом [563, с. 14].

А. Бернард відносить до інформаційної складової приватного життя: дані про події, пов'язані із тілом особи (дані про перенесені хвороби особи, які складають медичну таємницю); про терапевтичне або хірургічне лікування; смерть та долю людських останків; відомості про сімейне життя (за виключенням загальнодоступних даних); про факти приватних взаємин поза сімейним життям або розірвання відносин; внутрішні переконання особи (політичні або філософські погляди) [335, с. 160].

А. Уестін визначає право на інформаційну приватність як право особи приймати рішення, про ступінь відкритості та закритості по відношенню до зовнішнього світу, яку інформацію розкривати або залишити в таємниці [860, с. 168]. І. Альтман розвиваючи ідеї А. Уестіна, визначає приватність як важливий регуляторний динамічний процес, який безперервно змінює кордони особи з огляду на її взаємовідносини з навколишнім світом. Тож задовольняюча особу приватність є визначення бажаного балансу між «відкритістю-закритістю», «я та інші», «минуле та майбутнє» [297, с. 27]. Межі приватності не є абсолютними, а переважно обумовлюються обставинами, що мають розкриватися соціуму. Професор Р. Кларка визначив недоторканність приватного життя як право особи на особистий простір, вільний від втручання інших осіб та організацій, та сформулював чотири сфери приватності: фізична; поведінкова; комунікаційна; недоторканність персональних даних [435].

Визнаючи існування різноманітних підходів до розуміння інформаційної приватності, ми дотримуємося позиції, за якою інформаційна приватність

розуміється як право особи контролювати обсяг, зміст інформації, мету, способи пов'язані зі збором, обробкою та використанням персональних даних, незалежно від того, які дані збираються про фізичну особу, приватними та державними установами. При розкритті права на інформаційну приватність, необхідно враховувати, що зміст суб'єктивного права будучи сукупністю можливостей (правомочностей) складає правомочність на власні дії, тобто можливість самостійно здійснювати юридично та фактично значущі дії; правомочність вимагати від зобов'язаного суб'єкта виконання покладених на нього обов'язків; правомочність на захист, тобто можливість використання чи можливість вимагати використання державно-примусових заходів у випадку порушення суб'єктивного права.

Згідно з положеннями ст. 271 ЦК України, зміст особистого немайнового права становить можливість фізичної особи вільно, на власний розсуд визначати свою поведінку у сфері свого приватного життя. Одним з основоположних прав кожної людини є право отримувати, збирати, поширювати та використовувати інформацію. Кожна із зазначених правомочностей має свої особливості регулювання, які встановлюються залежно від умов їх здійснення та спрямованості на задоволення потреб людини у використанні такого блага. Так пошук інформації як процес визначається в доктрині шляхом вчинення дій із звернення особи до певного органу, установи чи іншого суб'єкта за отриманням необхідної інформації. Одержанням особистих чи публічних відомостей вважається перехід до такого запитувача у володіння та утримання необхідних йому даних від персони, яка володіє ними на законних підставах.

На наш погляд, при розкритті змісту права на інформаційну приватність, слід враховувати положення ст. 8 Закону України «Про захист персональних даних» та Регламенту ЄС 2016/679 (ст. 13, 14, 15, 16, 17, 18, 20, 21, 22), які передбачають низку прав, якими наділено суб'єктів персональних даних та кореспондуючі ним обов'язки контролера або процесора, серед яких: право на інформацію про обробку персональних даних та право на доступ до персональних даних; право на уточнення даних; право на видалення даних або

право бути забутим; право на обмеження обробки персональних даних; право на перенесення персональних даних; право не бути об'єктом автоматизованого прийняття рішення та право на захист від автоматизованого рішення, яке має правові наслідки; право на заперечення проти обробки персональних даних; право знати механізм автоматизованої обробки персональних даних. Як нам уявляється, означені правомочності змісту права на інформаційну приватність можна розглядати як самостійні права.

Відтак права на інформаційну приватність можна визначити як особисте немайнове право особи, контролювати обсяг та зміст інформації, пов'язаної зі збором, обробкою, поширенням та використанням персональних даних; правомочність вимагати від суб'єктів господарювання та органів державної влади виконання їх обов'язків щодо здійснення суб'єктом його правомочностей доступу до персональних даних, уточнення даних, видалення даних, обмеження обробки персональних даних, перенесення персональних даних; не бути об'єктом автоматизованого прийняття рішення, заперечення проти обробки та обмеження обробки персональних даних, знати механізм автоматизованої обробки даних; захист у разі незаконного збору, обробки, зберігання персональних даних та вимагати застування державно-примусових заходів у разі порушення суб'єктивного права. Здійснення правомочностей інформаційної приватності може бути розглянута за трьома критеріями і трьома можливостями поведінки.

Недоторканність приватного життя, інформаційна приватність зокрема, є не абсолютною категорією, з юридичної точки зору, як будь-яке суб'єктивне право є обмеженим публічними інтересами, правом на вираження поглядів, іншими правами, та з соціологічної точки зору, через зміну цінностей суспільства у бік відкритості. Парламентська Асамблея Ради Європи в п. 11 Резолюції Право на приватність № 1165 (1998) наголошує, що право кожної людини на приватність і право на свободу вираження поглядів є основою демократичного суспільства; ці права не є абсолютними і не мають ієрархічного характеру, оскільки мають однакову цінність [139].

Слід назвати існування таких об'єктивних чинників, які обумовлюють зміщення балансу приватності в мережі в сторону більшої відкритості. Перший чинник пов'язаний з фундаментальними змінами в суспільній свідомості та формуванням нової системи пріоритетів та цінностей. Другий чинник обумовлений розвитком інформаційно-комунікаційних технологій, які надають можливості дистанційного контролю за суспільством та життям фізичних осіб. Взаємодія цих чинників підвищує можливості зовнішнього впливу на приватне життя фізичних осіб та потребує суворого дотримання меж дозволеного втручання у приватне життя.

Користувачі в мережі прагнуть до більшої відкритості, що обумовлено здійсненням права на свободу вираження, використання цифрових платформ для просування товарів, робіт та послуг. Тож суспільство за допомогою власного комп'ютера щоденно себе оцифровує, в чому проявляється нищівне ставлення до права на приватність. З огляду на те, що фізичні особи не здатні діяти економічно раціонально щодо приватності та своїх персональних даних, оскільки на прийняття рішення про розкриття даних впливає низький рівень обізнаності та когнітивні неточності. С. Коколакіс запропонував ідею «парадокса приватності» [602, с. 123]. Відповідно ідеї науковця, особи фактично здатні та готові розкривати значно більший обсяг персональної інформації, ніж мають намір розкрити, що полягає в розбіжності між декларованою та фактичною поведінкою[538]. Дослідження підтверджує факт, що більшість фізичних осіб висловлює стурбованість відносно безпеки своїх персональних даних, поряд із тим продовжує розкривати більше даних. Слід погодитися з твердженням Д.Дж. Солове, що ризикована поведінка фізичних осіб при розкритті даних може бути обумовлена нездатністю та обізнаністю грамотного управління власною приватністю [796, с. 5].

Другий чинник обумовлений розвитком інформаційно-комунікаційних технологій, які надають ширші можливості для контролю за життям фізичних осіб. Всеохоплюючий інтернет та прискорення темпів конвергенції між фізичним та віртуальним світами ставить питання перегляду існуючого балансу

між приватним та публічним у житті фізичної особи. Торкаючись питань обмежувальних засад та пошуку балансу між недоторканністю приватного життя та суспільних інтересів слід зазначити, що виклик ставить розвиток IoT, обробка персональних та метаданих автоматизованими системами, всеохоплююче відеоспостереження, біометрична дистанційна ідентифікація тощо. До того ж як було з'ясовано вище, розуміння приватності відрізняється в державах з огляду на різноманіття підходів до правового регулювання інтернету [756]. Наразі в інтернеті під впливом транскордонності відбувається зміщення балансу між категоріями відкритості та закритості в бік прозорості інформації про фізичну особу. Якщо у фізичному світі дотримання умов приватності, як дотримання певних меж (соціальних, особистих або фізичних) передбачає існування реальної або уявної роздільної межі, то у віртуальному середовищі розуміння меж та кордонів досить розпливчасте. Змінюється ставлення осіб до таких категорій як «дистанція», «територіальність», «особистий простір», а налаштування конфіденційності особистого акаунту в соціальних мережах створюють хибне враження персонального середовища, оскільки дані акаунту та особисті вподобання фізичної особи стають відомими цифровим платформам та соціальним мережами. Умови конфіденційності в соціальних мережах є відносними, адже дозволяють обмежити доступ користувачів до перегляду акаунту, залишаючись «відкритим» для платформи.

Як свідчать результати проведеного у 2006 році експерименту організацією AOL, яка публікувала пошукові запити за минулі року, щоб надати учасникам проєкту можливість дослідити їх. Маючи доступ до 650 тис. анонімізованих даних користувачів (IP користувачів, ім'я, час пошуку були замінені індивідуальними числовими ідентифікаторами), співвставивши окремі запити за кілька днів, учасники ідентифікували окремих користувачів [325]. Наразі результати опитувань свідчать, що суспільство очікує: розкриття все більшого масиву персональних даних державним органам та корпораціям, які мотивовані у їх використанні; приватність стане прерогативою окремих осіб, які

володіють ресурсом для захисту від всеосяжного спостереження; забезпечення безпеки персональних даних ускладниться [650].

Як констатує Ю.С. Размєтаєва, відзначаються дві тенденції: тенденція до відкритості та деанонімізація в публічному віртуальному просторі й тенденція зростаючого накопичення різноманітних даних про особу у глобальних та локальних інформаційних мережах [175, с. 43].

На погляд А. де Хінг, в умовах набуття персональними даними властивостей об'єктів цивільного обігу, підхід до регулювання приватності та захисту персональних даних поступово зміщується в бік обмеження приватності [562, с. 1280].

З погляду В.М. Брижко, В.Г. Пилипчука, гарантії забезпечення умов приватності стосовно персональних даних є не абсолютними, істотно залежать від контексту, яким визначаються норми захисту приватного життя й вимоги того, що може бути розкрите для публічності або держави. Межі інформаційної приватності є рухливими та особа за її бажанням вирішує, яку інформацію повідомляти про себе [14, с. 34]. П.Д. Гуйван зазначає, що складовою приватного життя особи є елементи інформаційного права особи, які можуть мати як ознаки приватності, так і прояви публічного характеру. При цьому їх розмежування є досить умовним, оскільки людина може розцінювати деякі аспекти трудової участі, навчання та інших проявів суспільної діяльності як складові свого особистого життя[48, с. 180]. Науковець звертає увагу на значущість балансу приватних та суспільних інтересів, розроблених у практиці ЄСПЛ. З одного боку, особа наділена правом на повагу приватного та сімейного життя за ст. 8 ЄКПЛ, водночас може виникати потреба в обмеженні права в разі пріоритету суспільного інтересу та потребі забезпечення права на доступ до публічної інформації за ст. 10 ЄКПЛ.

Через конкуренцію, з одного боку, інтересів особи в захисті недоторканності приватного життя та персональних даних, з іншого боку, інтересів суспільства в обробці персональних даних у публічних інтересах, на державу покладається обов'язок визначення та дотримання балансу інтересів.

Поряд із позитивним обов'язком держави гарантувати повагу до прав закріплених у ст. 8 ЄКПЛ, держави несуть негативні зобов'язання. ЄСПЛ у своїх рішеннях наголошує, що обмеження права недоторканності приватного життя має провадиться на підставі закону, мати легітимну мету та бути необхідною в демократичному суспільстві[406].

Слід зазначити, що у практиці ЄСПЛ межі позитивних та негативних зобов'язань держав передбачені ЄКПЛ не визначені однозначно ясно, а можна лише простежити в нерозривній єдності із застосуванням принципів. Під час вирішення спору, Суд враховує справедливий баланс, який необхідно досягти під час порівняння конкуруючих інтересів окремої особи та суспільства загалом, та на який поширюється наданий державі вільний розсуд.

Обмеження здійснення права на інформаційну приватність та окремих правомочностей фізичних осіб передбачені ст. 23 Регламенту ЄС 2016/679. Права суб'єктів даних можуть бути обмежені в разі: існування загроз інтересам національної, громадської безпеки та оборони; запобігання, розслідування, виявлення та переслідування кримінальних злочинів або виконання кримінальних покарань, у тому числі протидії загрозам громадської безпеці та їх запобіганню; важливих цілей загального публічного інтересу ЄС чи держав-членів, зокрема економічних чи фінансових інтересів, включаючи грошові, бюджетні та податкові питання, соціальну охорону здоров'я та громадську безпеку; захисту незалежності судової влади та захисту судочинства; попередження, розслідування, виявлення та переслідування порушень етичних норм окремих професій; моніторингових, контрольних та регулятивних функцій, пов'язаних із здійсненням повноважень публічної влади; захисту суб'єктів даних або прав та свобод інших осіб; виконанням судових рішень.

Регламент ЄС 2016/679 передбачає, що нормативно-правовий акт, який обмежує здійснення прав фізичних осіб, має містити спеціальне застереження щодо: мети обробки та категорії персональних даних, які оброблюються; обсяг введеного обмеження; гарантії проти зловживання або несанкціонованого доступу або передачі даних; визначення контролерів; строків зберігання та

застосування гарантій, з урахуванням обсягу та цілі обробки, категорії даних; ризиків для прав та свобод суб'єктів даних; права суб'єктів даних на отримання інформації про обмеження його прав, у тій мірі, яка не шкодить меті обмеження.

В умовах поширення IoT, актуальною є проблема дотримання приватності та повсюдного відеоспостереження. Відеозаписи з камер відеоспостереження можуть бути носіями персональних даних, у разі застосування автоматизованих технології розпізнавання обличчя та віддаленої біометричної ідентифікації. Наразі лідером використання технології відеоспостереження із дистанційним біометричним розпізнаванням є КНР, де технології віддаленої біометричної ідентифікації активно застосовуються та експортується[249]. Технологія передбачає присвоєння особі балів та рейтингу в системі, може відправляти дані правоохоронним органам про те, що особа має неоплачені штрафи, ухиляється від сплати аліментів або перебуває в розшуку [196]. Технологія дозволяє уряду КНР збирати великі обсяги даних про громадян.

Проєкт iBorderCtrl використовує штучний інтелект на зовнішніх кордонах ЄС, який передбачає складання профіля мандрівника на основі комп'ютерного автоматичного інтерв'ю, зафіксованого камерою мандрівника перед мандрівкою, та аналізу штучним інтелектом 38 мікро жестів. Впровадження технології знаходиться на етапі тестування в Угорщині, Латвії та Греції [737].

Наразі технологія відеоспостереження із дистанційним біометричним розпізнаванням допомагає правозахисним організаціям виявляти жертв работоргівлі, визначати їх місцезнаходження. Наприклад, компанія Marinus Analytics використовує програму в сервісі Amazon Rekognition [613].

Європейський парламент закликає заборонити використання приватних баз даних розпізнавання обличчя, таких як Clearview AI правоохоронними органами. Водночас у зв'язку з введенням в Україні воєнного стану та вчиненням воєнних злочинів, Україні було надано доступ до приватної бази даних Clearview AI, яка містить майже десять мільярдів фотографій, що дозволяє перевіряти фізичних осіб при перетині кордону [288]. Як зазначає, український правник Г.А. Мамедов, додаток Clearview AI допомагає правоохоронним органам

України в ідентифікації потенційних злочинців та загиблих [100]. Крім того, українські правоохоронні органи під час проведення розслідувань порушень міжнародного кримінального та гуманітарного права, керуються вимогами ведення розслідувань з використанням відкритих цифрових даних та інформації з відкритих джерел, передбаченими Протоколом Берклі, який затверджений Управлінням Верховного комісара ООН [168]. Правоохоронні органи США використовували Clearview AI для встановлення учасників масових заворушень під час протестів Black Lives Matter та штурму Капітолію у Вашингтоні[34]. Clearview AI відома тим, що надає послуги державним органам та його представникам. База фотографій збирається із відкритих джерел, соціальних мереж в інтернеті, зокрема громадян ЄС, що відповідно порушує законодавство ЄС щодо отримання законної згоди на збір та обробку персональних даних [233, с. 3].

Позитивний вплив від застосування систем віддаленої біометричної ідентифікації в області правозастосування, підвищення ефективності роботи правоохоронних та судових органів в області боротьби зі злочинністю визнає Європарламент у Резолюції від 6 жовтня 2021 р., водночас технологія несе ризики використання для масового спостереження, що не відповідає засадам демократичного суспільства [701].

Європейська Рада з питань захисту персональних даних констатує високі ризики шкоди від застосування технологій розпізнавання обличчя [834]. Адже всеосяжне відеоспостереження технологій IoT може впливати на психіку, здійснення прав та вимагає дотримання законодавства про захист персональних даних. До того ж поширення технології ставить питання етико-правових засад її поширення та застосування.

Використання систем біометричної ідентифікації вимагає дотримання принципу законності, оскільки залишаються ризики вторинного використання даних, зібраних системами відеоспостереження, яке порушує мету, для якої вони були отримані та зібрані. Залишаються сумніви ефективності застосування технології, адже відеоспостереження не запобігло вчиненню терористичних

актів у громадському транспорті в Лондоні [643], терористичних актів 11 вересня 2001 року в США. К. Веліз підтверджує, що використання систем відеоспостереження неефективне в попередженні терористичних актів, оскільки вони є не закономірними вчинками, а умисним порушенням законодавства. До того ж втручання у приватне життя, яке справляє відеоспостереження, також може призводити до загибелі людей [824].

Тому поряд із позитивним ефектом від використання технології дистанційним біометричним розпізнаванням, наразі відзначається розробка виваженого підходу у правовому регулюванні та встановлення чітких правових підстав використання технології. Компанія Facebook у 2021 році відмовилася від використання технології розпізнавання обличчя, у зв'язку із побоюванням з боку користувачів та вірогідністю накладенням штрафних санкцій[738]. Не можна виключати, що таке рішення прийняте через скандали щодо порушення законодавства про захист персональних даних компанією в ЄС [3]. КНР поступово запроваджуються законодавчі обмеження використання технології. Згідно зі ст. 26 Закону КНР Про захист персональної інформації, що набрав чинності 1 листопада 2021 року, передбачено, що встановлення обладнання для збору зображень або розпізнавання обличчя у громадських місцях повинно здійснюватися у випадках, коли це вимагається засадами національної та громадської безпеки та згідно з законодавством, про що має бути чітко зазначено. Збір зображень та індивідуальних ідентифікаційних ознак може здійснюватися тільки з метою національної безпеки, та не може здійснюватися для іншої мети, за виключенням наданої згоди суб'єкта даних [739].

Простежується певна тенденція обмеження використання систем відеоспостереження з дистанційним розпізнаванням обличчя у США та окремих штатах у діяльності правоохоронних органів. Влітку у 2020 році до Конгресу США було внесено законопроєкт про запровадження мораторію на використання технологій розпізнавання обличчя та біометричних технологій [818]. На рівні штатів подібні акти ухвалено в Іллінойсі, Техасі, Каліфорнії, Вашинґтоні [499], Колорадо та Арканзасі [508], штаті Мен[534; 651], Сан-

Франциско, Окленді [449; 527]. Водночас обмеження використання технології обумовлені потребою її вдосконалення, через виникаючі випадки помилкового розпізнавання людей, що призводить до дискримінації. Крім того, постає питання щодо делегування рішень та функцій автоматизованим системам у воєнній сфері, де обговорюється необхідність встановлення заборони на використання воєнних роботів, які можуть приймати повністю автоматизовані рішення щодо життя і смерті людини[432, с. 2]. У цьому сенсі, правозахисна організація Amnesty International висловлює занепокоєння використання систем розпізнавання обличчя та введення заборони на їх використання [324].

Вельми лояльну позицію, яка відрізняється від досить суворої позиції ЄС, відносно використання систем дистанційної біометричної ідентифікації займає Великобританія. Занепокоєння про застосування спостереження, збір та обробка персональних даних державною (п. 88) висловив голова Верхового Суду Великобританії у справі T & Anor, R (on the application of) v Secretary of State for the Home Department & Anor [413]. У Великобританії застосування систем біометричної ідентифікації відбувається під наглядом таких незалежних органів як: Офіс уповноваженого з питань інформації та Уповноваженого з питань відеоспостереження та біометричних даних.

Апеляційний Суд Англії та Уельсу у справі Bridges, R (On the Application Of) v South Wales Police (England and Wales Court of Appeal, EWC) розробив низку критеріїв та гарантій, яким повинно відповідати використання систем розпізнавання для того, щоб бути визнаним законним. Позивач у справі стверджував, що дистанційне розпізнавання обличчя порушує ст. 8 ЄКПЛ та обов’язок державних органів забезпечувати фізичними особам дотримання рівних можливостей відповідно до Закону Великобританії Про рівність 2010 [502]. Суд визнав незаконним і таким, що порушує ст. 8 ЄКПЛ, використання систем автоматичного розпізнавання обличчя за відсутності чіткої вказівки законодавства, місцерозташування, де може відбуватися застосування таких систем. Суд зазначив, що законодавство передбачає, що місце повинно бути таким, в якому на розумних підставах передбачається присутність людей,

включених до баз даних (списку спостереження). У свою чергу, залишати вирішення таких питань на розсуд правоохоронних органів є неприпустимим [404].

Суд, однак, визнав практику використання систем дистанційного розпізнавання обличчя такою, що відповідає критерію пропорційності, якщо її функціонування побудовано відповідно до послідовних етапів біометричного розпізнавання обличчя алгоритмом (етапи розпізнавання розглянуті у Підрозділі 2.4. «Ідентифікуючі ознаки фізичної особи у відносинах у мережі «Інтернет»).

Відповідно у Великобританії забороняється розпізнавання широкого кола осіб та вимагається обмежувати переліком осіб, які перебувають у розшуку. Заборонено створення та зберігання баз даних про переміщення фізичних осіб. Дані з камер зовнішнього відеоспостереження не можуть використовуватися для невибіркового розпізнавання осіб, об'єднання в єдину базу даних та підлягають автоматичному видаленню протягом місяця з моменту запису.

Традиційно досить послідовну позицію в питанні правового регулювання прав та свобод фізичних осіб, та функціонування новітніх інформаційно-комунікаційних технологій, у тому числі технологій дистанційної біометричної ідентифікації займає ЄС. Відповідно до Резолюції Європейського парламенту від 6 жовтня 2021 р. щодо штучного інтелекту у кримінальному праві та його використання поліцією та судовими органами у кримінальних справах, людина не лише має право на правильну ідентифікацію, а й право взагалі не бути ідентифікованою, за виключенням випадків, коли це вимагається законодавством у зв'язку із суспільними інтересами (п. 8)[701]. Безумовно в сучасних реаліях реалізувати дане положення є доволі складним.

За твердженням Верховного комісара ООН з прав людини М. Башлет, у доповіді від 13 вересня 2021 р. «Право на недоторканність приватного життя в цифрову епоху», посилаючись на ст. 2 і 17 МПГПП [105] на держави покладається не лише обов'язок не порушувати фундаментальне право людини на недоторканність приватного життя («негативний обов'язок»), а й «позитивний обов'язок» захищати осіб від подібних посягань та дискримінації,

в межах своєї юрисдикції, зокрема встановлювати належні правові гарантії та інструменти для їх ефективної реалізації (п. 10 Доповіді) [319]. Дистанційне біометричне розпізнавання обличчя, згідно з М. Башлет, пов'язане з істотним втручанням у приватне життя. Біометричні дані є одним з ключових ідентифікаторів особи, які дозволяють відрізнити особу від решти. Використання дистанційної біометричної ідентифікації підвищує можливість державних органів систематично провадити ідентифікацію та спостереження за людьми в громадських місцях, підриваючи право людина на недоторканність приватного життя та негативно впливаючи на такі права як свобода думки, свобода мирних зібрань і об'єднань та свобода пересування (п. 27 Доповіді).

Резолюція Європарламенту Про штучний інтелект у кримінальному провадженні та його використанні поліцією і судовими органами у кримінальних справах від 6 жовтня 2021 р. також наголошує, що повсюдне використання технологій віддаленої біометричної ідентифікації торкається права на людську гідність, що становить основу всіх основних прав, гарантованих Хартією ЄС про основні права [426]. Використання і збір будь-яких біометричних даних для цілей віддаленої ідентифікації, наприклад, шляхом розпізнавання обличчя у громадських місцях, а також на автоматичних контрольно-пропускних пунктах, які використовуються для прикордонного контролю в аеропортах, може складати високі ризики для основоположних прав, наслідки яких можуть значно варіюватися залежно від мети, контексту і сфери використання [701]. У Резолюції Європарламент дотримується позиції про те, що впровадження систем ШІ у правоохоронній та судовій сферах має розглядатися не як звичайна технічна можливість, а як рішення, яке впливає на здійснення прав та свобод людини, ефективне здійснення кримінального судочинства. Використання систем біометричної віддаленої ідентифікації правоохоронними органами має бути обмежене чітко обґрунтованими цілями, за умови дотримання принципів пропорційності та необхідності. Використання технології має відповідати вимогам дотримання принципів обробки, таким як мінімізація даних, точність даних, обмеження строків зберігання, забезпечення безпеки даних і підзвітність,

а також бути законною, справедливою та прозорою, та переслідувати конкретну мету, чітко визначену законодавством.

Дистанційне відеоспостереження та ідентифікації вимагає проведення оцінки наслідків впровадження технологій, які знижують роль людини у правозастосуванні та винесенні судових рішень, адже фактично ставить виклик існуючому підходу реагування на правопорушення після вчинення, не припускаючи, що кожна особа потребує постійного нагляду та спостереження для превенції правопорушень.

Означена ситуація призводить то того, що внаслідок використання технології розпізнавання обличчя, особа жодним чином не впливає на обсяг даних, які збираються відносно неї, що посягає на її інформаційне самовизначення, людську гідність та недоторканність приватного життя. За таких умов розширення застосування технологій відеоспостереження може здійснювати вплив на прийняття рішення особами не лише у сфері щоденних правочинів, а й політичного вибору. Крім того, цілі заради яких розширюється застосування відеоспостереження, можуть так і залишитися недосяжними, а втручання у приватне життя буде невідворотно порушено.

Оскільки застосування технології відеоспостереження із дистанційним біометричним розпізнаванням являє собою обробку персональних даних, то застосування технології вимагає дотримання принципів обробки персональних даних, принципу законної обробку та застосування технології лише за умови, якщо це необхідно для досягнення законної мети обробки.

Згідно з Керівництвом 2/2019 Європейської ради із захисту персональних даних щодо обробки персональних даних відповідно до статті 6(1)(b) Регламенту ЄС 2016/679 зазначено, що в контексті надання онлайн-послуг суб’єктам даних «необхідність» позначає неможливість досягнення мети іншим способом. Йдеться саме про неможливість досягти мети, а не про вартість або зручність тощо. Необхідність має бути наявною, реально існуючою або вона має виникнути в найближчому майбутньому, а не гіпотетичною. Обробка

персональних даних «на випадок» для досягнення гіпотетичної мети, яка вірогідно не настане, не охоплюється категорією «необхідність» [713; 715].

Суд ЄС у справі Heinz Huber v Bundesrepublik Deutschland зазначив, що концепт «необхідності» має незалежне значення у праві ЄС, яке має тлумачитися в повній відповідності до цілей законодавства про захист персональних даних [388].

У справі Valsts policijas Rigas regiona parvaldes Kartibas policijas parvalde v. Rigas pasvaldibas SIA Rigas satiksme Суд ЄС застережив, що відступи та обмеження стосовно обробки персональних даних можуть застосовуватися лише, якщо це суворо необхідно [414]. ЄКПЛ у ч. 2 ст. 8 наголошує, що органи державної влади не можуть порушувати недоторканність приватного життя інакше як: на підставі закону; якщо це необхідно в демократичному суспільстві в інтересах національної безпеки, громадської безпеки та економічного добробуту держави, для запобігання або припинення злочину, захисту здоров'я чи моралі або захисту прав і свобод інших осіб. У ч. 1 ст. 52 Хартії ЄС про основні права міститься аналогічне формулювання, однак його доповнює принцип пропорційності, під яким розуміється пропорційність між характером запроваджуваних обмежень та впливом на права суб'єктів, з одного боку, і важливістю та масштабом переслідуваних цілей, з іншого.

Саме з посиланням на ст. 8 ЄКПЛ заявники у справі Szabó and Vissy v. Hungary [411] звернулися до ЄСПЛ та скаржилися на те, що відносно них можуть бути застосовані потенційно невиправдані та непропорційні міри начебто для забезпечення безпеки, обґрунтовані застосуванням заходів антитерористичного характеру. Служба національної безпеки Угорщини використовувала заходи спостереження, прослуховування записів телефонних розмов, перевірку змісту електронних повідомлень без відома осіб, за якими здійснюється спостереження. Суд визнав надмірність заходів спостереження, порушення статті 8 ЄКПЛ та відсутність проведеної оцінки необхідності такого спостереження та судового нагляду за цією діяльністю. Тож мало місце необмежене втручання органів державної влади у приватне життя фізичних осіб.

Використання систем дистанційної біометричної ідентифікації залишається предметом дискусій. Напередодні прийняття Акту ЄС про штучний інтелект Європейська Рада із захисту персональних даних та Європейський наглядовий орган із захисту персональних даних дали Висновок, в якому рекомендували запровадження загальної заборони на будь-яке використання ШІ для дистанційного розпізнавання осіб у загальнодоступних місцях. Відповідно до Висновку зазначено, що дистанційна біометрична ідентифікація осіб у громадських місцях несе високі ризики втручання у приватне життя осіб, може зачіпати людську гідність [717]. У Висновку обґрунтовувано, що використання автоматизованих систем може порушувати дотримання пропорційності, через можливу обробку даних невибіркової та невідповідної кількості суб'єктів даних для ідентифікації лише декількох осіб (наприклад, пасажирів в аеропортах та вокзалах). Безконтактний характер систем дистанційного відеоспостереження з біометричним розпізнаванням обличчя вимагає дотримання прозорості та правових підстав для обробки даних, належного інформування осіб про відеоспостереження. Адже застосування подібних систем істотно впливає на дотримання засад (розумного) очікування анонімності у громадських місцях та може негативно впливати на здійснення таких прав та свобод людини як свобода вираження поглядів, зібрань та пересування. Застосування технології не відповідає вимогам необхідності та пропорційності, що випливає з розуміння допустимого втручання у фундаментальні права, як це тлумачить Суд ЄС та ЄСПЛ.

Аналогічна позиція була висловлена Європейським парламентом у Резолюції Про штучний інтелект у кримінальному провадженні та його використанні поліцією та судовими органами у кримінальних справах від 6 жовтня 2021 р. Європейський парламент рекомендував запровадити постійну заборону на використання автоматизованого розпізнавання в публічно доступних місцях рис людини, таких як хода, відбитки пальців, ДНК, голос та інші біометричні та поведінкові дані. Було рекомендовано запровадити мораторій на впровадження систем розпізнавання обличчя з функціями

ідентифікації у правоохоронних цілях, якщо тільки вони не використовуються для ідентифікації постраждалих від злочинів. Умовою запровадження технології також є дотримання прав людини, отримання неупереджених та недискримінаційних результатів, недопущення зловживання та суворого демократичного контролю й нагляду.

Врешті окремі рекомендації були взяті до уваги та прийнятий Акт ЄС про штучний інтелект від 13 березня 2024 року, який повністю заборонив та відніс до технологій із високим ризиком: системи, які впливають на думку виборців під час проведення політичних перегонів (використання систем ШІ, які застосовують методи впливу на підсвідомість, виходять за межі свідомості людини або з маніпулятивним наміром, або оманними методами з метою істотного спотворення поведінки людини); рекомендаційні алгоритми, які використовуються соціальними мережами із кількістю більше 45 млн. користувачів; технології розпізнавання обличчя у громадських місяцях у режимі реального часу, системи розпізнавання емоцій у використанні правоохоронними органами (в тому числі прикордонний контроль), в тому числі роботодавцями та навчальними закладами до категорії технологій із високим рівнем ризику для прав і свобод людини та встановлення загальної заборони на використання таких технологій, за виключенням чітко визначених випадків; системи соціального рейтингу (оцінки). Забороняється застування прогностичних систем правоохоронними органами, які використовують штучний інтелект для аналізу великих даних та виявлення на їх підставі потенційних правопорушників або жертв.

Слід зазначити, що спірні положення Проєкту Акту ЄС про ШІ щодо біометричної ідентифікації в публічних місцях були предметом обговорень коаліції правозахисних організацій Європи та США, та здавалися узгодженим в результаті кропіткої роботи, однак в останню мить були внесені зміни, які нівелювали низку домовленостей. Акт ЄС про ШІ передбачає ретроспективне розпізнавання, тобто використання технології розпізнавання обличчя не в режимі реального часу, а розпізнавання обличчя на раніше записаних

відеоматеріалах без рішення суду [313]. За твердженням правозахисників, подібне положення не відповідає попереднім заявам Єврокомісії та Європарламенту про те, що розпізнавання обличчя має проводитися за умови суворих гарантій та має бути дозволена лише в окремих виключних обставинах та лише за рішенням суду.

На наш погляд, будь-які спроби запровадити в законодавстві повну заборону на впровадження біометричних технологій, у тому числі застосування системи віддаленої біометричної ідентифікації, з огляду на ризик порушення фундаментальних прав, невдоволення суспільства, наразі не зупинить розвиток технологій та науковий прогрес. Потребує розробка адекватного та ефективного правового регулювання використання технологій, беручи до уваги комплекс підходів, що включає технічні, організаційні, методичні та правові заходи, засади захисту прав та законних інтересів фізичних осіб, несанкціонованого втручання у приватне життя та інших загроз, зловживань, пов’язаних із незаконним втручанням у приватне життя, що вимагає досягнення балансу між інтересами держави в забезпеченні суспільного порядку та інтересами приватних осіб у запобіганні втручанні в їх приватне життя. Крім того, Акт ЄС про ШІ поширюється на українські компанії які розробляють ШІ рішення та працюють на ринку ЄС[64].

З огляду на удосконалення інформаційно-комунікаційних технологій та мережі, розвиток систем ШІ, який має відбуватися на принципах відповідальності, підзвітності, антропоцентричності та заслуговуючих довіри систем ШІ. Застосування систем віддаленої біометричної ідентифікації має бути обмеженим та включати такі складові як: заборона на використання систем розпізнавання приватними компаніями у громадських місцях; заборона на невибіркове розпізнавання осіб та обмеження лише особами, які перебувають у розшуку, встановлення підстав і процедури внесення осіб до переліку розшукуваних; визначення місць розміщення систем розпізнавання обличчя, інформування про використання відеоспостереження у публічних місцях; механізми здійснення та захисту прав особами; заборона встановлення

прихованого відеоспостереження; встановлення граничних строків зберігання даних. Чітке визначення відповідальності державних органів, уповноважених на використання систем розпізнавання.

Слід зазначити, що в Україні наразі бракує належного правового регулювання використання технологій віддаленої біометричної ідентифікації. У Верховній Раді зареєстровано Проєкт Закону «Про єдину систему відеомоніторингу стану публічної безпеки» № 11031, який передбачає, що ідентифікація фізичної особи має здійснюватися на підставі набору даних: імені; дати народження або смерті; місця народження; статі; даних про зареєстроване місце проживання (перебування) особи; відомостей про громадянство; відцифрованого образу обличчя особи; реєстраційного номера облікової картки платника податків, номера транспортного засобу тощо[29; 141]. Для ефективного впровадження технологій, система відеомоніторингу стану публічної безпеки має отримати доступ до Єдиного державного демографічного реєстру, Єдиної інформаційно-аналітичної системи управління міграційними процесами, національної системи біометричної верифікації тощо. Напередодні Міністерство внутрішніх справ анонсувало запуск більше 50 тисяч камер відеоспостереження, в тому числі з функціями розпізнавання обличчя [28].

Слід зазначити, що даний Проєкт Закону потребує ґрунтовного доопрацювання. Значні ризики, пов’язані з впровадженням систем дистанційної біометричної ідентифікації, з потенційними порушеннями значного переліку прав людини у зв’язку зі здійсненням розпізнавання фізичних осіб. При запровадженні систем віддаленої біометричної ідентифікації законодавцем має оцінюватися вплив впровадження технології на: право на недоторканність приватного життя, право на повагу приватного та сімейного життя, свободу вираження поглядів, свободу зібрань та об’єднань, право на справедливий суд, недопущення дискримінації та ін. Проєкт Закону не містить розуміння етапів використання біометричної ідентифікації, включаючи етапи створення баз даних, що порушує принцип прозорості обробки персональних даних. В даному випадку доцільно звернутися до судової практики Великобританії, де

розроблена покрокова процедура створення баз даних та проведення дистанційної ідентифікації. Проєкт Закону не говорить про те, чи система зможе проводити невибіркове або нецільове розпізнавання обличчя шляхом розширення баз даних за рахунок зображень облич із мережі «Інтернет» або інших приватних баз даних, що є забороненим відповідно до Акту ЄС про ШІ. Не вбачаються чіткими зі змісту Проєкту Закону – чи технології розпізнавання зможуть функціонувати в режимі реального часу (аналогічно практиці КНР), чи передбачається ретроспективне розпізнавання обличчя за матеріалами відеозаписів. Слід звернути уваги, як це було зазначено вище, дане положення є вкрай важливим, в Акті ЄС про ШІ звертається увага на заборону використання систем дистанційної біометричної ідентифікації в режимі реального часу в публічних місцях для правоохоронних цілей за виключення окремих ситуацій. Акт ЄС про ШІ допускає розпізнання в режимі реального часу із врахуванням конкретної ситуації та оцінки наслідків використання системи для прав та свобод усіх зацікавлених осіб. Проєкт Закону не містить підстав або випадків обробки чутливих даних, до яких відносяться біометричні дані. Поряд із цим, Конвенція 108 та Регламент ЄС 2016/679 зазначає, що обробка біометричних даних може бути дозволена, якщо вона ґрунтується на відповідній правовій підставі, та якщо відповідні гарантії закріплені у законодавстві. Крім того, Проєкт Закону не передбачає створення та функціонування незалежного наглядового органу (омбудсмена), уповноваженого здійснювати контроль за функціонуванням систем відеоспостереження. Потребує також врегулювання застосування механізмів захисту зібраних персональних даних. Підхід для правового регулювання використання технологій штучного інтелекту та віддаленої біометричної ідентифікації в Україні має враховувати вплив запровадження технології на фізичних осіб, високі ризики втручання у приватне життя та враховувати досвід ЄС в даному питанні. Одним із таких кроків, вважаємо має стати, запровадження в законодавстві повної заборони на проведення невибіркового або нецільового розпізнавання обличчя шляхом розширення баз уданих за рахунок зображень облич із мережі «Інтернет», приватних баз та

створення об’єднаних баз даних, використання технології для впливу на підсвідомість для підбурювання до певної поведінки, прийняття рішень та застосування систем соціального рейтингу (оцінки).

Окремо слід зупинитися на тому, що підключення камер відеоспостереження до мережі «Інтернет» (системи IoT в цілому) залишає ризики несанкціонованого доступу до камер зловмисниками. Подібні ризики пов’язані з доступом третіх осіб до камер, підключених до мережі «Інтернет», існують постійно, через що на контролерів покладаються обов’язки впроваджувати заходи захисту персональних даних з огляду на поточний рівень розвитку науково-технічного прогресу. Відповідно до ст. 25 Регламенту ЄС 2016/679, передбачено вимоги створення систем із вбудованим захистом персональних даних та систем приватності за замовчуванням – Privacy by design та privacy by default. Вбудована приватність передбачає, що контролер даних зобов’язаний вбудувати систему захисту даних (у тому числі у процеси розробки продукту або послуги) на ранніх етапах їх проєктування та зобов’язаний підтримувати таку систему безперервно в подальшому. За задумом, вбудована приватність даних є обов’язком заздалегідь передбачити захист персональних даних у всіх діях, починаннях та рішеннях компанії. Наприклад, під час проєктування та розробки мобільного додатку необхідно проаналізувати та попередити вірогідні ризики, пов’язані з конфіденційністю, та встановити механізми управління такими ризиками ще до написання програмного коду. Провідна ідея «вбудованої приватності» в тому, що для мінімізації ризиків, пов’язаних з конфіденційністю, – найкраще не створювати їх.

Конфіденційність за замовчуванням передбачає, що користувачі не мають вживати жодних заходів та дій для захисту своєї приватності. Налаштування із дотримання умов приватності та захисту персональних даних мають встановлені за замовчуванням розробником. Збиратися мають лише ті дані, які необхідні для досягнення конкретної мети обробки. Наприклад, при збиранні даних, необхідних для реєстрації користувача, додаток не повинен затребувати надання даних, які не є необхідними для проведення реєстрації. Тому чим менше

компанія збирає та обробляє даних, тим нижчою є вірогідність порушення нею Регламенту ЄС 2016/679.

Вважається, що розробка концепції вбудованої приватності та приватності за замовчуванням належить Е. Кавукян, спеціально уповноваженої з питань приватності та захисту персональних даних провінції Онтаріо, в Канаді [420]. Е. Кавукян запропонувала такі принципи, які мають брати до уваги компанії: превентивні заходи, а не лише усунення наслідків; приватність за замовчуванням; вбудована приватність; повна функціональність за взаємною згодою; захист персональних даних упродовж всього циклу їх збору, зберігання, обробки та знищення; доступність та прозорість; повага до приватності користувачів (система має бути зорієнтованою на користувачів). На погляд Е. Кавукян, контролери зобов'язані розглядати питання конфіденційності даних протягом всього життєвого циклу даних, тобто з початку проєктування програми (продукту). Вбудована приватність забезпечує безперервне та безпечне управління життєвим циклом даних від початку обробки до завершення. Конфіденційність за замовчуванням означає, що принцип вбудованої конфіденційності має бути застосований щодо всіх систем таким чином, щоб дані захищались від дій третіх осіб. Тобто користувачі не зобов'язані вживати жодних зусиль для захисту недоторканності свого життя.

Аналіз ст. 25 Регламенту ЄС 2016/679 зокрема дозоляє говорити, що під час розробки товару має враховуватись критерій рівня науково-технічного розвитку (state of art) для забезпечення належної безпеки програми (товару) та найбільш ефективного досягнення мети обробки. Згідно зі ст. 25, зазначається про витрати на впровадження заходів безпеки, що має тлумачитися поширювально, включати не лише фінансові витрати, а й витрати часу та ресурсів людини. Слід зазначити, що під витратами на впровадження заходів безпеки розуміється впровадження ефективних та адекватних мір захисту, та не вимагає застосування високих за вартістю. Відповідно до ст. 42 Регламенту ЄС 2016/679 передбачено застосування сертифікації, яка є свідченням дотримання принципів вбудованої приватності та приватності за замовченням.

Тож із прийняттям Регламенту ЄС 2016/679, на контролерів було покладено значний тягар, пов'язаний із забезпеченням вбудованої приватності та приватності за замовчуванням. З метою дотримання положень ст. 25 Регламенту ЄС 2016/679 та уникнення значних штрафних санкцій, контролери мають аналізувати процес обробки та вживати заходи, щоб право на приватність суб'єктів забезпечувалось на кожному етапі обробки, починаючи від процесу проєктування та розробки програм (товару). Підсумовуючи викладене, можна назвати такі заходи, які мають здійснити контролери: розробка програм конфіденційності для компанії, що визначає кожен етап на якому обробляються дані, та гарантує, що всі відділи (департаменти володіють організаційними заходами, планом захисту персональних даних); мінімізація обробки персональних даних (обробка має здійснювались лише тих даних, які дійсно необхідні контролеру для досягнення мети обробки); розробка плану захисту персональних даних як частини будь-якої підприємницької діяльності; застосування псевдоанімізації або шифрування даних, якщо такі заходи можливі; забезпечення прозорості будь-якої обробки персональних даних та інформування суб'єктів даних про їх використання; забезпечення суб'єктам даних можливості здійснення їх прав; бути обізнаними щодо рівня розвитку технологій (state of art) у сфері захисту персональних даних, новітніх засобів захисту; відстежувати рекомендації державних органів, уповноважених у сфері захисту персональних даних.

Підсумовуючи викладене, можна стверджувати, що сьогоднішній світ стає схожим на «семантичне павутиння» або «безшовну мережу всіх даних життя людини». Взаємодія між новітніми технологіями, IoT, автоматизованими системами та забезпеченням інформаційної приватності є складними та багатогранними. Новітні технології продовжують невідворотно, змінювати різні аспекти буття людини. Провідні виклики обмовлені невпинним зростанням масштабів даних, які збирають компанії, що викликає побоювання поступового та непомітного розгортання цифрових диктатур. Беручи до уваги, що зупинити розвиток технологічного прогресу неможливо, провідна роль та відповідальність

за розробку виважених людиноцентристських підходів за дотриманням прав людини покладається на правників.

3.3.2. Право на доступ до мережі «Інтернет»

Для здійснення прав в інтернеті, особі необхідно мати відповідний доступ до нього, що ставить безпосередньо питання нерівності в доступі до інтернету, цифрової нерівності та цифрового розриву[53, с. 69]. У 2010 році Х. Клінтон наголошувала, що свобода підключення аналогічна свободі зібрань лише в кіберсередовищі, дозволяє людям виходити в онлайн, спілкуватися та співпрацювати, а уряд не має перешкоджати підключенню до інтернету [765].

Наразі майже всі держави члени ООН розвивають національні електронні сервіси державних послуг, перелік яких розширюється [490]. Проте із зростанням прозорості діяльності держаних органів, зростає «цифровий розрив» та цифрова нерівність як різновид соціальної нерівності, що виражається в обмеженні окремих осіб, груп внаслідок відсутності доступу до сучасних засобів комунікації. За твердженням С. Рейнхордаса, через перехід державних послуг в онлайн значне коло осіб виключається, а цифрова нерівність не лише відтворює існуючу соціально-економічну нерівність, а й стає самостійним джерелом відчуження [761, с. 4]. У рейтингу готовності держав до мережевого суспільства, який щорічно вираховується міжнародною організацією «Всесвітнього економічного форуму» та спільно з Міжнародною школою бізнесу Said, Україна займає найвищі показники серед держав з доходом нижчим за середній [684].

Винайдення інтернету, з одного боку, дозолило подолати монополію традиційних ЗМІ, з іншого боку, технологічне відставання окремих держав та концентрація переважної кількості розробників програмного забезпечення, дослідницьких інститутів, інфраструктури у США обумовило поглиблення «цифрового розриву» між технологічно розвинутими державами та державами, які розвиваються, та між населенням за інтелектуальної ознакою, тими хто має доступ та належні компетенції, високі доходи та зрештою, що впливає та високий попит на фахівців у галузі інформаційних технологій та розривом у доходах населення [505]. Спалах пандемії COVID-19 прискорив перехід більшості видів діяльності в дистанційну форму, від освітніх послуг, культурних заходів, до

юридичних послуг та судочинства [102, с. 59; 127, с. 65]. Разом з цим, пандемія поглибила масштаби цифрового розриву між розвиненими державами (багатими) та державами, які розвиваються (бідними), та усередині цих держав.

Відповідно до Доповіді Спеціального доповідача ООН Ф. Ла Рю, позбавлення держав, які розвиваються, доступу до інтернету ставить їх в несприятливе становище, що поглиблює нерівність серед населення держав та між окремими державами[614]. Як зазначає О.І. Гапченко, високорозвинені держави акумулюють провідні технології, досягнення у сфері науки та техніки, та їх вклад перевищує досягнення держав, які розвиваються [33, с. 186]. Адже вплив глобалізації на розвиток держав та розподіл технологій є не лінійним, а провідні новітні технології залишаються прерогативою розвинених держав [229, с. 123]. Високо розвинуті держави ладні витрачати значні ресурси на розвиток освіти, науки, законодавчо забезпечувати ефективний захист авторів об'єктів інтелектуальної власності та можливість відстоювати свої права[219, с. 54]. Висловлюється думка, що для забезпечення доступу до інтернету, розвинені (заможні) держави мають допомогти державам, які розвиваються, для скорочення цифрового розриву.

Е. Чедвік та К. Мей наголошують, що кожна модель взаємодії держави та населення вимагає забезпечення доступу осіб до технологій та інтернету [422, с. 272].

Цифрова нерівність, будучи одним із провідних негативних наслідків інформаційного суспільства та цифрового розриву (поряд із економічною, расовою, гендерною нерівністю) є одним із різновидів соціальної нерівності та виражається в обмеженні окремих осіб, цивільних груп внаслідок відсутності доступу до сучасних засобів комунікації. Від доступу до інтернету залежить можливість здійснення інших прав людини.

Тлумачення сутності «розриву» в умовах цифровізації може означати позбавлення певних соціальних груп доступу до засобів комунікації та доступ до інтернету, в дискримінації осіб на тих, хто мають можливість бути учасниками відносин в інтернеті та тих, хто позбавлений такої можливості, вочевидь

стосується визначення правового статусу особи, що регламентується Конституцією України.

Стаття 24 Конституції України передбачає, що громадяни мають рівні конституційні права і свободи та є рівними перед законом [78]. У сучасних умовах конституційно-правова рівність осіб у здійсненні своїх прав можлива лише в разі рівного доступу осіб до інформаційно-комунікаційних технологій.

В умовах інформаційного суспільства значущими стають гарантії соціальної рівності, а принцип «цифрової рівності» має бути передбачений та забезпечений державними гарантіями. Уявляється доцільним включити до ст. 24 Конституції таку ознаку як доступ до інтернету та інформаційно-комунікаційних технологій, та гарантування державою рівності прав та свобод осіб незалежно від можливості доступу до інформаційно- комунікаційних технологій та доступу до мережі «Інтернет».

Аналіз міжнародно-правових актів, прийнятих ООН [124], ЮНЕСКО [763], ОБСЕ [664] та іншими міжнародними організаціями, дає підстави стверджувати, що розвиток концепції права доступу до інтернету відбувається в тісному зв’язку з правом вираження поглядів та правом на інформацію, оскільки відсутність доступу до технологій може позбавити можливості реалізувати цивільні права[138]. Огляд міжнародно-правових актів та Доповіді Ф. Ла Рю [614; 740, с. 10]свідчить, що більшість з них уникають визнання доступу до інтернету як права людини, а переважно називають його умовою або засобом здійснення особами своїх прав та свобод та розширення можливостей інтернету як засобу здійснення конституційних прав.

Л. Шошкевич висуває позицію, що міжнародно-правовою підставою доступу до інтернету слід розглядати підп. п. 1 ст. 15 Міжнародного пакту про економічні, соціальні та культурні права, який передбачає право кожної людини на користування результатами наукового прогресу та їх практичного застосування [790, с. 49]. Водночас означений аспект доступу до інтернету досі не отримав належного аналізу в доктрині та в актах міжнародних організацій.

Закріплення права на доступ до інтернету не отримало єдиного підходу щодо визнання на національному рівні. Можна виділити декілька підходів в оформленні прав на доступ до інтернету в різних державах: перший шлях пов'язаний із внесенням змін та закріплення у законодавстві права доступу до інтернету; другий шлях пов'язаний із внесенням змін до конституції; третій шлях обумовлений закріпленням права в рішеннях судових органів.

Перший підхід пов'язаний із внесенням змін у законодавство та віднесення доступу до інтернету до універсальних та загальнодоступних послуг, як це закріплено в законодавстві Естонії [809], Іспанії [627] та Італії [525, с.5]. Однієї із перших держав, яка закріпила у своєму законодавстві у 2000 році право доступу до інтернету як невід'ємного права 21-го сторіччя, була Естонія [836, с.178].

Другий підхід пов'язаний із внесенням змін до конституції. Так, Греція взяла на себе обов'язок спростити доступ до передавання електричних сигналів інформації, а також можливості з її створення, обміну та поширення. Конституція Португалії передбачає положення, що кожному гарантується право на вільний доступ до загальнодоступних інформаційних мереж [442].

Третій шлях пов'язаний із закріпленням в актах судових органів. Конституційний суд Коста-Ріки від 18.06.2010 р. визнав доступ до інтернету невід'ємним засобом здійснення основних прав людини та зобов'язав державні органи підтримувати надання послуг зв'язку та користування мережею [546]. Конституційний суд Франції в рішенні від 10.05.2009 р. [468] фактично визнав доступ до інтернету однією з необхідних умов здійснення свободи вираження поглядів як права першого покоління.

З урахуванням зазначеного, розглянуті вище Конституції дотримуються підходу права доступу до інтернету як похідного права, від права на інформацію.

Рада Європи у прийнятих документах та рішеннях ЄСПЛ наголошує на обов'язку держав-членів забезпечувати кожному, хто перебуває в межах її юрисдикції, дотримання права та основоположних свобод. Так, ЄСПЛ розглядає право доступу до інтернету та захисту контенту в межах свободи вираження

слова та поглядів, відповідно до ст. 10 ЄКПЛ [77], ст. 19 ЗДПЛ та ст. 19 МПГПП (захист свободи думки та вираження).

Слід навести справу «Їлдирим проти Туреччини», де Суд зазначив, що інтернет став одним із основних засобів здійснення права на свободу вираження поглядів та свободи інформації [369]. Із рішення ЄСПЛ не вбачається визнання права на доступ до інтернету як нового фундаментального права. Суд дотримується похідного характеру прав на доступ до інтернету, виводячи його як похідного зі свободи вираження слова та поглядів.

У більш пізній справі Kalda v. Estonia щодо надання особам які відбувають покарання права доступу до інтернету, ЄСПЛ розглянув справу в контексті права на інформацію за ст. 10 ЄКПЛ. Позивач вимагав, від адміністрації закладу відбування покарання, надати доступ до: онлайн версії державної газети, рішень судів, бази даних із рішеннями ЄСПЛ. Суд у своєму рішенні наголосив про необхідність забезпечення державами права доступу до інтернету для ефективного подолання цифрового розриву[390]. Суд зазначив про право осіб отримувати інформацію, яка становить загальний інтерес. Рішення ЄСПЛ було піддано критиці через ризик стати прецедентом, надання, особам які відбувають покарання, права вимагати доступу до інтернету та покладання на державу обов'язку забезпечення здійснення права, що обумовлене додатковими витратами.

У справі Jankovskis v. Lithuania про відмову адміністрації в'язниці надати доступ до інтернету заявник звернувся до Міністерства освіти щодо можливості навчанні в університеті та отримав відповідь про можливість ознайомлення з усією необхідною інформацією на сайті [389]. Адміністрація закладу відбування покарання відмовила в доступі до інтернету, у зв'язку з тим, що на заявника не поширюються діючі правила в'язниці. Поряд з відмовами попередніх інстанцій надати доступ до інтернету, ЄСПЛ зазначив прагнення засудженого отримати вищу освіту, сприяє досягненню мети ресоціалізації, а тому не має обмежуватися, а сучасний процес навчання вимагає доступу до інтернету.

На погляд А. Лепаж, право на доступ до інтернету слід розглядати як соціальне право або як індивідуальну вимогу до держави, подібно до таких послуг як освіта, охорона здоров'я та соціальне забезпечення. Це універсальна послуга, яку державні органи повинні гарантувати своїм громадянам шляхом інвестування державних ресурсів, соціальної та освітньої політики. Фактично доступ до інтернету та ведення бізнесу через інтернет є засобами, за допомогою яких люди вступають у відносини з державною владою, тобто здійснюють свої права [635, с. 56].

Слід констатувати, що попри транскордонний характер, саме держава в особі державних органів, впливає на вільний доступ до мережі «Інтернет», обирає підходи до правового регулювання мережі та визначає ступінь проникнення інтернету в суспільство та життя людей. Так, у КНР впроваджено інтернет цензуру та обмеження доступу до соціальних мереж та платформ таких як: Google, Facebook, YouTube, Instagram, Twitter, Wikipedia, сайту міжнародної правозахисної організації Amnesty International, ресурсам різних іноземних ЗМІ (The New York Times, The Independent, Bloomberg, BBC) та інших. Державна інтернет цензура діє в разі виявлення ключових слів, які знаходяться в «чорному списку». У консервативному Ірані від початку інтернет розвивався вільно, водночас у подальшому був суворо обмежений, особливо внаслідок масових протестів у 2009 році [808].

В. Володавська вважає, що право на доступ до інтернету має базуватися на принципах: інклюзивності та недискримінації, мережевої нейтральності, гарантування безпечності інтернету та гарантованої якості сервісу [25]. В умовах воєнного стану та регулярних аварійних відключень електроенергії, світла та тепла для технічних умов доступу до електроенергії та інтернету, органи державної влади та місцевого самоврядування в Україні забезпечують функціонування пунктів із відповідними послугами для населення [170].

Можна виділити два підходи до правового регулювання доступу до інтернету: інструментальний та правовзахисний. Прибічники інструментального або технологічного підходу дотримуються точки зору на інтернет як засіб

(інструмент) здійснення прав на доступ до інформації та вираження поглядів. Прибічники правозахисного підходу, переважно представники юридичної спільноти, відстоюють позицію, що доступ до інтернету характеризується власним юридичним змістом та має зайняти місце з-поміж інших прав людини [110, с. 77; 208 с. 53]. У літературі висловлюється позиція визнання права на доступ до інтернету як фундаментального права [257], існує інша позиція про співвідношення права на доступ до інтернету з іншими правами, а саме, правом на інформацію.

Розгляд інтернету як технології, яка допомагає здійсненню прав людини, переважно властивий фахівцям у галузі технологій та програмістам. За твердженням В. Серфа, одного із розробників мережі «Інтернет», мережа є лише технологічним засобом, існування якої не впливає на наявність або відсутність прав людини, а права людини не повинні пов'язуватися із існуванням певної технології. Інтернет, який виник на певному етапі розвитку суспільства та на його місце може прийти інший засіб. В. Серфа порівнює інтернет із конем, що на певному етапі людині було важко обійтись без коня, але з цього не слідує, що слід визнавати право людини на коня [421]. Аналогічної позиції дотримується Л. Лессіг [636; 637, с. 501].

Визнані права людини мають механізм правозастосування, а поспішне впровадження нових прав людини може призвести до фрагментації прав, на погляд Ф. Істербрука, а поглиблення в деталі може призвести до появи «права на коня». Ф. Істербрук, будучи деканом Чиказької школи, виступав проти викладання курсу «право на коня» на факультеті, маючи на увазі ІТ право, а лише викладання фундаментальних юридичних дисциплін [489, с. 207]

Визначення як права всього «бажаного та привабливого» може призвести до «інфляції прав» та підриву ядра прав людини, який підлягає захисту, девальвації права, а цінності прав людини як таких, оскільки не всі держави ладні забезпечити здійснення прав на доступ до мережі. Аналогічно застережує про інфляцію прав та зменшення цінності решти існуючих прав Ф. Кунер, а

включення нових прав у систему прав є виправданим у разі існування додаткової цінності в захисті даного права [607, с. 307]

На погляд Дж. Томальті, доступ до інтернету не може бути визнано універсальним природним правом, яке належить всім людям, тому що природа людини не передбачає доступу до інтернету, людина жила без доступу до мережі без шкоди для себе всі ці часи, та можливо зможе обійтися без нього в майбутньому, у випадку винайдення ефективніших технологій [830, с. 6].

З урахуванням вищезазначеного, система прав є не статичною, еволюціонує, відображає розвиток суспільства та цінностей. Можна провести порівняння, як на певному етапі розвитку прав, право на інформацію набуло свого місця повноцінного права в системі прав людини, наразі дискутують стосовно місця права на доступ до інтернету серед прав людини.

Успіх поширення використання інтернету пов'язаний із відкритістю його архітектури та, зокрема, розподільчими властивостями мережі [579, с. 47]. Спочатку інтернет був створений як середовище, вільне від національних кордонів та державно-правового регулювання, як зазначає Л. Гернсі [547]. За твердженням Дж. П. Барлоу [327, с. 5], В. Маккінзі [649, с. 35] інтернет за задумом створювався як простір вільного обміну інформацією [579, с. 47]. М. Марчук дотримується позиції: визнання права доступу до інтернету як базового права людини, яке має гарантуватися державою поряд із правами людини [101, с. 116].

Існують позиції науковців визнання права на доступ до інтернету в межах та широкого тлумачення існуючих прав як свободи вираження поглядів та права на інформації[735, с. 108]. Б. Калі[361, с. 276], О. Полічіано [744], С. Тьюлі [836, с. 175], Д. Джойс [587, с. 493], Дж Торнхіл [826], М. Реглітц [764, с. 314], Б. Бест[338, с. 23], аргументом на користь визнання права на доступ називають вагоме значення інтернету для людини, її особистого розвитку та участі в житті суспільства та економіці, заснованій на знаннях. Наступним аргументом називається неможливість повною мірою реалізувати інші права, зокрема свободу вираження поглядів, право на зібрання в інтернеті, право на освіту [336,

с. 42], як наприклад, під час пандемії COVID-19. Проблема, яка загострилася в різних регіонах світу через відсутність покриття [428]. Л. Жасмонтайта та П. Де Герта, називають аргументом на користь підтримки зростаючого кола осіб, які користуються послугами електронного урядування та потребують доступу до мережі[581, с. 18]. Занепокоєння щодо обтяжливості для держав забезпечення підключення до мережі можна спростувати аргументом Б. Калі, що жодне право не є абсолютним, і до прав доступу до інтернету слід застосовувати загальні обмеження: обов'язки поступової реалізації, мінімальні основні зобов'язання та пріоритетність надання, та доступ вразливим членам суспільства (особам похилого віку, інвалідам та ін.)[361, с. 276]. Дж. Кюлінг та К. Нейман вважають, що уряди держав можуть розділити витрати на забезпечення покриття між суб'єктами приватного сектору шляхом укладення спільної домовленості та співпраці [605, с. 201]

Аналіз позицій науковців та міжнародно-правових актів дозволяє виділити два напрями здійснення права доступу до інтернету: 1) доступ до інтернет-інфраструктури, або право на підключення (право на вхід) до інтернету, в межах якого інтернет розглядається в контексті послуги; 2) доступ до контенту, який створюється та поширюється в мережі, право на комунікацію в широкому значення (включаючи право шукати, отримувати, створювати та передавати контент користувачам), та право не бути відключеним від інтернету, під яким розуміється недопущення незаконного блокування доступу до сайтів.

У кожному з означених напрямів можна виділити низку окремих правомочностей носіїв суб'єктивного права [599]. Право суб'єкта на доступ до інтернету передбачає наявність у нього таких складових правомочностей як: правомочність володіння та користування електронними пристроями для доступу до інтернету (вибору пристрою), доступу до таких пристроїв за розумною ціною та без дискримінації; правомочність на приєднання до інфраструктури інтернету за допомогою доступу до послуг провайдера зв'язку за розумною ціною та недопущення дискримінації; правомочність обирати та вільно використовувати правомірно поширюване програмне забезпечення;

право на особисту безпеку, збереження недоторканності приватного життя, збереження особистої, сімейної та іншої таємниці, а також таємниці кореспонденції під час електронних комунікацій (здійснення доступу до інтернету має не обмежувати здійснення даних прав, вони мають однаково реалізовуватись та захищатися в онлайн та офлайн).

Право доступу до контенту, який створюється та поширюється за допомогою інтернету, реалізується за рахунок таких правомочностей як: вільний пошук та отримання інформації, правомірно поширюваної в мережі; створення та поширення інформації в інтернет за умови дотримання встановлених обмежень із дотримання прав людини, недопущення дискримінації та ризику необґрунтованих переслідувань за переконання чи ідеї, що поширюються в інтернеті; участь у приватних електронних комунікаціях (один на один або визначеним колом осіб) за допомогою сервісів електронної пошти, відеоконференцій, месенджерів тощо, зі збереженням таємниці кореспонденції та недоторканності приватного життя; право на «цифрову ідентичність», яке включає право особи обрати ім'я, використовувати власне ім'я, псевдонім у мережі, відповідно до вимог законодавства чи виступати анонімно.

Доцільно зазначити, що здійснення окремих правомочностей може не забезпечуватися належними чином через відсутність єдності позицій держав стосовно розуміння юридичного змісту права доступу до інтернету. Відповідно у звіті ОБСЄ, лише 17 держав-учасниць закріпили у законодавстві права доступу до інтернету. До того ж розмежування здійснення «право на вхід» та «право на комунікацію» є умовною, оскільки взаємно обумовлюють один одного. По-перше, право на вхід не має значущості, якщо не пов'язано із подальшою комунікацію, спілкуванням, пошуком, отриманням та поширенням інформації. Адже вхід в інтернет здійснюється для подальшого вчинення дій, без яких вихід з інтернету втрачає значення. По-друге, вчинення комунікації, пошук в інтернеті не можливо реалізувати без попереднього здійснення «права на вхід». Тож здійснення «права на вхід» є необхідною передумовою здійснення «права на комунікацію».

Хоча обґрунтування визнання права на доступ до інтернету є досить дискусійним питанням, ми вважаємо, що ідея такого визнання є своєчасною. По-перше, підходи до правового регулювання, які використовуються в КНР, спрямовані на контролювання, цензурування та обмеження доступу до інтернету свідчать про зростаючу потребу в забезпеченні доступу та підтримання вільного інтернету. По-друге, розвиток концепції сервісно-орієнтованої держави та «paperless» створює умови, коли отримання переважної кількості послуг органів державної влади та місцевого самоврядування, доступу до судочинства та ведення переговорів стає найбільш ефективним саме в мережі «Інтернет». По-друге, стихійні лиха, епідемії, збройні воєнні конфлікти, міграція створюють передумови зростання обсягів залучення користувачів до цифрового середовища, як безпечного простору, вираження творчості, отримання освіти та спілкування.

Дотримуючись правозахисного підходу щодо визнання доступу до інтернету як права людини, дискусії надалі точаться щодо коректності визнання права доступу до інтернету як елемента інших прав або визнання його самостійним правом, навіть фундаментальним правом людини.

Т.І. Швидка вважає, що право на доступ до інтернету є самостійним, цілісним правом, невід'ємним від людини, може забезпечуватися державою, водночас тісно пов'язаним з іншими правами та свободами людини. Поряд з цим, здійснення зазначеного права безпосередньо залежить від фінансових ресурсів держави, різниці в кількості населення та території, що ускладнює можливість розробки єдиного світового стандарту, який мали б забезпечувати держави [281, с. 145]. Право доступу до інтернету як елемента інших прав людини, дотримується О.А. Гончаренко [44, с. 23]. Дана думка спирається на ідею, що право на інформацію, право на вираження поглядів та вираження творчості реалізується переважно за допомогою доступу до інтернету. Наразі доступ до інтернету відіграє провідну роль у здійсненні означених прав людини та є складовою цих прав.

Визнаючи наявність власного юридичного змісту, що полягає в наборі правомочностей особи, постає питання, чи дозволяють перелічені правомочності віднести право доступу до інтернету до фундаментальних прав людини, поставивши його поряд з іншими загальновизнаними правами і свободами, що є вельми дискусійним, адже не будь-яке суб'єктивне право може визнаватися як таке. А закріплення існуючого каталогу прав людини у ЗДПЛ та надалі у відповідних пактах про права людини є результатом тривалих дискусій та компромісів. Так, І.В. Мукомела дотримується позиції, що право на доступ до інтернету є фундаментальним правом людини [110, с. 77].

Науковцями право на доступ до інтернету переважно розглядається як похідне право від інших прав, визнаних міжнародною спільнотою, а аргументами проти такого визнання називають наступне: не характеризуватися власним унікальним юридичним змістом, з тим не вносить до переліку основоположних прав людини якісно нового змісту, може випливати з інших фундаментальних прав, а його юридичний зміст може поєднувати правомочності, які складають вміст інших прав, що свідчить про його похідний характер. Вичерпних критеріїв для відмежування фундаментальних прав людини від інших прав не розроблено в науці. За твердженням винахідника інтернету В. Серфа, право на доступ до інтернету обмежений певним етапом розвитку цивілізації, та не належало кожній особі у всі часи.

Зміст права на доступ до інтернету можна визначати через інші складові права людини, які характеризуються власним змістом. Так, «право на вхід» до інтернету може бути розглянуто як синтез права на інформацію (ст. 19 МПГПП), право використовувати досягнення технологічного прогресу (ст. 15 МПГПП) та право на стандарти життя, необхідні для підтримки здоров’я та добробуту (ст. 25 ЗДПЛ), та право на недоторканність приватного життя тощо.

Право на доступ до інтернету порівнюється із правом на питну воду, яке гарантується конституціями держав Африки та Азії, проте не визнається фундаментальним правом[667]. Як зазначає К. Матієсен, попри те, що право на питну воду визнано Генеральною Асамблею ООН, воно залишається похідним

від права на гідний рівень життя, право на рівність та заборону дискримінації. Аналогічно праву на вільний друк, передбаченим у ст. 19 МПГПП та інших міжнародних актах, є похідним від свободи вираження поглядів [656, с. 9].

Визнаючи значущість доступу до інтернету в сучасному суспільстві, можна констатувати, що інтернет ще не перетворився у життєво необхідну умову існування людини як питна вода, а закріплення права доступу до інтернету в законодавстві автоматично не створить покриття в місцях, де воно фактично відсутнє. Можна припустити, що глобальний космічний інтернет як Starlink от SpaceX, зможе забезпечити сигнал у кожному куточку на землі[832].

Щодо питання доцільності законодавчого закріплення права на доступ до інтернету в Україні, то на наш погляд, запровадження такої норми в законодавстві має стати поштовхом для створення ефективної системи здійснення прав та свобод у цифровому середовищі, а держава має взяти на себе обов'язок здійснення права.

Закон України «Про електронні комунікації» передбачає права, обов'язки та відповідальність фізичних осіб та постачальників електронно-комунікаційних послуг. У п. 80 ст. 2 Закону України «Про електронні комунікації» дано визначення послуги доступу до мережі «Інтернет» як електронно-комунікаційної послуги, що забезпечує доступ до мережі «Інтернет» та можливість з'єднання з кінцевими точками мережі «Інтернет» незалежно від технології, що застосовується в електронній комунікаційній мережі, та кінцевого (термального) обладнання, що використовується[153]. Відповідно до ст. 124 Закону України «Про електронні комунікації», передбачається захист інтересів кінцевих користувачів у разі припинення постачальником електронних комунікаційних послуг діяльності з надання таких послуг у вигляді покладення обов'язку на постачальника електронних комунікаційних послуг, попередити кінцевих користувачів не пізніше ніж за три місяці до припинення надання електронних комунікаційних послуг.

За ст. 105 Закону України «Про електронні комунікації» передбачено обов'язок постачальників електронних комунікаційних послуг надання

інформації про: заходи, вживані постачальником, які можуть впливати на якість послуг доступу до мережі «Інтернет» та можливий вплив на конфіденційність та захист персональних даних кінцевих користувачів; вплив обмежень обсягу, швидкості та інших параметрів якості на послугу доступу до мережі «Інтернет», зокрема на використання контенту, програм та послуг; мінімальну, середню та максимальну швидкість передання даних до мережі «Інтернет», або прогнозування максимальної швидкості завантаження на пристрій та завантаження до мережі «Інтернет» при мобільному зв'язку, та вплив відхилень від заявленої швидкості здійснення прав кінцевих користувачів стосовно отримання послуги.

Майнову відповідальність постачальників електронних комунікаційних послуг перед кінцевими користувачами за ненадання або неналежне надання електронних комунікаційних послуг передбачено ст. 125 Закону України «Про електронні комунікації».

Проєкт Закону № 4715 від 16.04.2014 «Про внесення доповнень до ЦК України (щодо гарантування права фізичної особи на доступ до інтернету)», планував доповнити ЦК України статтею 302-1 «право на доступ до інтернету», яка б передбачила право фізичної особи на доступ до інтернету, який не може бути обмежений, а обмеження доступу можливе щодо певних даних, що містяться в інтернеті, лише на підставі рішення суду про незаконність таких даних». Проєкт Закону розглядав право на доступ до інтернету як ключову свободу в умовах інформаційного суспільства, проте його не було прийнято[142].

У свою чергу, ч. 2 ст. 18 Закону України «Про електронні комунікації» передбачає умови та обов'язки постачальників електронних комунікаційних мереж та/або послуг дотримуватися правил загальної авторизації та підстави обмеження своїх абонентів до ресурсів за рішенням суду, обмежувати доступ до сайтів, визначених уповноважених органом, та інші підстави обмежень.

Здійснення права доступу до інтернету не може бути зведена до здійснення традиційних фундаментальних прав, вимагає активної участі держави та

виконання її позитивних гарантій, оскільки полягає не лише в набутті суб'єктом додаткових інструментів для входу до інтернету, та не може бути реалізована без активних дій держави, таких як забезпечення підключення до мережі, якщо в місцевості немає необхідної інфраструктури. Для того, щоб скористатися інтернетом, має бути забезпечений мінімальний рівень підключення. Тому Ла Рю нагадує про позитивне зобов'язання держав заохочувати та сприяти здійсненню права на свободу вираження поглядів та запровадження заходів, необхідних для здійснення цього права, в тому числі забезпечення підключення до мережі «Інтернет»[614; 615].

Здійснення правомочностей доступу до інтернету потребують дотримання негативних гарантій з боку держави: невтручання у сферу приватного життя, відмова від непропорційного та безпідставного обмеження, недопустимість масового відключення інтернету та блокування доступу до ресурсів (якщо такі блокування виходять за межі допущених міжнародно-правовими актами), недопущення переслідування користувачів в інтернеті за політичні висловлювання, переконання та погляди в мережі, (журналістів, блогерів) та ін. Тож дотримання таких гарантій залежить від політичного курсу в державі. Як приклад, відключення інтернету або уповільнення його функціонування (застосовується в період виборчих перегонів та масових заворушень), сувора фільтрація контенту і блокування сторінок зарубіжних держав, кримінальне переслідування активістів в Ірані, КНР та ін.

Право на доступ до мережі «Інтернет» передбачає існування негативних та позитивних гарантій, спрямованих на надання всім особам без дискримінації можливості підключення до мережі. Оскільки в умовах суворих обмежень «права на комунікацію», здійснення «права на вхід» може обмежити можливість належного здійснення прав у мережі. Протилежне натомість є актуальним, якщо держава не гарантує здійснення «права на вхід» у мережу, негативні гарантії «права на комунікацію» (невтручання у права та свободи) та вільний обмін даними в інтернеті залишаються нереалізованими.

Декларація ОБСЕ «Про свободу вираження поглядів в інтернеті» 2011 року передбачає позитивні обов'язки держав забезпечувати доступ максимально широкого кола користувачів до інтернету. Серед таких обов'язків: визнання доступу до інтернету як права людини та визнання невід'ємною складовою компонента права на вільне вираження поглядів та свободу інформації; дотримання мережевого нейтралітету; уникнення «аварійного» відключення інтернету; відмова держав-учасниць ОБСЄ від обов'язкового блокування контенту або сайтів, через негативний вплив на свободу вираження та вільний потік інформації; прозорість та передбачена законом можливість оскарження механізму добровільного блокування та видалення контенту; дотримання принципу «вільний доступ»; дотримання принципу «свобода вираження»[524]. Відповідно Обсяг позитивних гарантій, як правило, зумовлений наявністю у кожної конкретної держави відповідних матеріальних ресурсів, а також доступністю на тій чи іншій території необхідної інфраструктури зв'язку, що обслуговується провайдерами.

Отож, право доступу до інтернету слід визнавати правом, яке складається з правомочностей: доступ до інфраструктури мережі або право на підключення (право на вхід) до інтернету, в межах якого інтернет розглядається в контексті послуги; доступу до контенту, який створюється та поширюється в мережі, право на комунікацію в широкому значенні (включаючи право шукати, отримувати, створювати та передавати контент користувачам), якому кореспондує обов'язок держави забезпечувати здійснення права доступу до мережі та комунікацію, не відключати від інтернету, не застосовувати незаконного блокування сайтів. Наразі право на доступ до інтернету не визнається як фундаментальне право, водночас по мірі залучення кількості користувачів не виключено, що може перестати розглядатися як похідне право від права на інформацію.

Слід зазначити, що аналіз вищезгаданих нормативно-правових актів дозоляє стверджувати, що на міжнародному рівні не передбачається належних гарантій здійснення права на доступ, документи носять декларативний характер.

У свою чергу, на рівні держав розробляються нормативно правові акти для гарантування здійснення права на доступ.

Сучасне життя без використання інтернету повинно було б збідніти, водночас для встановлення обмежень нав'язливого та всеохоплюючого інтернету в доктрині та законодавстві закріплюються положення, спрямовані на забезпечення прав та гарантій найманих працівників. Потреба зменшення тиску всеохоплюючого інтернету, забезпечення охорони праці та прав найманих працівників, виключати засоби комунікації в неробочий час обумовили виникнення та розвиток права на офлайн або право на відключення (право перебувати в автономному режимі). Поштовхом для розробки даних норм стала пандемія Covid-19 та поширення інформаційно-комунікаційних технологій поряд із покращенням умов найманих працівників. З одного боку, виникали виклики стирання кордонів між робочим та вільним часом, з іншого, виник ризик надмірного перевантаження з огляду на постійне перебування в мережі інтернет. Означене негативно впливає на психологічний, емоційний, фізичний стан та ефективність, виконуваних обов'язків працівників[788, с. 1975]. Тому провідною тенденцією правового регулювання трудових відносин у світі стало забезпечення стабільного балансу між робочим та позаробочим часом в умовах цифровізації.

Слушною в цьому аспекті є думка Е. Кастронова – що розглядаючи права аватарів, агенти мають володіти правом залишати віртуальні світи та входити до них за власним бажанням [419, с. 37]. Про зміну цінностей та пріоритетів у повсякденному житті, втрату демаркаційної лінії між приватним та публічним, вільним та робочим часом, що смартфон на відпочинку став необхідною складової життя, – звертає увагу З. Бауман[5, с. 51].

Вперше згадування про право на відключення було в рішенні Палати з трудових спорів Верховного Суду Франції ще у 2001 році. У 2004 році Верховний Суд підтвердив свій висновок в іншому рішенні, зазначивши, що той факт, що працівник не був на телефонному зв'язку в неробочий час, не може розглядатися як порушення трудової дисципліни. Означені рішення вплинули на регулювання трудової діяльності та у 2017 році набули чинності зміни до

Трудового кодексу Франції, які закріпили право найманих працівників на відключення та захист свого позаробочого вільного часу. Компанії з п’ятдесятьма працівниками та більше зобов’язані укласти угоди зі своїм персоналом щодо годин, в які роботодавець має право зв’язатися з ними. Поза цими годинами роботодавець не має права зв’язуватися не особисто, не по телефону або електронною поштою. Таким чином, найманим працівникам право бути офлайн, принаймні у трудовій сфері. У Франції це право отримало назву як право на відключення (droit à la déconnexion) [629]. Право на відключення також набуло закріплення в законодавстві Італії, а в Німеччині Міністерство зайнятості заборонило керівникам зв’язуватися з працівниками у вільний від роботи час. У грудні 2020 року Європейський парламент закликав закріпити «права на відключення» в законодавстві всіх держав членів ЄС, принаймні частково в рамках перспективи поширення Covid-19, під час якої все більше людей стало працювати віддалено вдома.

Метою якого було врегулювання дистанційної роботи, право на відключення було закріплено Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення правового регулювання дистанційної, надомної роботи та робити із застосуванням гнучкого робочого часу» від 04.02.2021 № № 1213-IX[147]. Даний Закон доповнив Кодекс Законів про працю статтею 60-2 [86], яка передбачила поняття «період відключення» для працівника, який виконує дистанційну роботу, в даний проміжок часу гарантується вільний час для відпочинку (період відключення), під час якого працівник може переривати будь-який інформаційно-телекомунікаційний зв’язок з власником або уповноваженим органом, та це не визнається порушенням умов трудового договору або трудової дисципліни. Вільний період часу для відпочинку (період відключення) визначається у трудовому договорі про дистанційну роботу. Дана норма є переважно декларативною, оскільки не містить конкретних санкцій та запобіжних заходів. Аналіз норм законодавства дозволяє стверджувати, що в теорії скористатися правом на відключення працівник може і зараз, адже за ст. 31 Кодексу законів про працю власник або

уповноважений ним орган не має права вимагати від працівника виконання роботи, не обумовленої трудовим договором. Отже, якщо, наприклад, на підприємстві встановлено доволі стандартний графік роботи з 09:00 до 18:00, то працівник може не відповідати на робочі дзвінки або електронні листи починаючи з 18:01 [89].

З погляду Б. Кастерса, право на офлайн слід розглядати як більш ширше право в порівнянні з правом на відключення, перебування в автономному режимі, яке має поширюватися на різні сфери життя та не обмежуватися лише трудовими відносинами [447, с. 4]. Право на відключення або перебування в автономному режимі слід відмежовувати від права на недоторканність приватного життя у значенні як «право бути залишеним у спокої». Концепція останнього розроблена в англосаксонській правовій доктрині, в тому числі обробки персональних даних відповідно до Регламенту ЄС. Суб'єкт може вживати заходи для недопущення незаконного збору та обробки його персональних даних в мережі, використовувати засоби анонімізації, водночас це позбавляє його надмірного перебування в мережі.

Право на офлайн піддається критиці через те, що не є вільним вибором фізичної особи. Право на відключення або право на офлайн має розглядатися у нерозривному зв'язку із правом на доступ до інтернету [556, с. 1996]. Разом з цим, з урахуванням посилання проникнення технологій у сучасне життя, право на офлайн має забезпечити додатковий захист від втручання у приватне життя.

Підсумовуючи викладене, слід зазначити, що здійснення права на доступ до інтернету не можна звести лише до здійснення традиційних прав людини, та воно полягає не просто в набутті особи додаткових інструментів для пошуку інформації. Право доступу до інтернету характеризується власним юридичним змістом, який полягає в низці правомочностей суб'єкта. Окрім юридичного змісту, право доступу до інтернету характеризується власною цінністю, яка проявляється в долученні суб'єкта до світової глобальної спільноти. З огляду на різний обсяг гарантій доступу до інтернету, передбаченого в законодавствах

різних держав, стає актуальним розробка стандартів доступ до Інтернету на міжнародному рівні.

3.3.3. Окремі цифрові права

З огляду на повсюдне проникнення інформаційно-комунікаційних технологій, зростає значущість довіри до них, постає потреба розробки технологічно відкритих способів обробки даних. До того ж цінність та роль персональних даних в уявленні суспільства безповоротно змінюється. Зібрані персональні дані та отримані на їх підставі результати аналітики більше не можуть розглядатися як об'єкти права власності корпорацій, які ними маніпулюють та використовують без погодження із суб'єктами даних. Поряд із цим, поширення застосування систем автоматизованого прийняття рішень в економічній галузі, державних послуг, заснованих на технологіях аналізу великих даних та системах ШІ, дозволяє зберегти людський ресурс та покликані підвищити ефективність прийняття рішень.

Здійснення права на інформацію та доступ до персональних даних слід розділити на: інформування суб'єкта даних контролером на початку збирання персональних даних (дані можуть бути відібранні як від суб'єкта даних, так і від третьої сторони ст. 13, 14 Регламенту ЄС 2016/679) та право суб'єкта на доступ до власних даних, які вже збираються (ст. 15 Регламенту ЄС 2016/679).

На контролера відпочатку збору персональних даних покладається низка обов'язків щодо повідомлення суб'єкта даних про отримання персональних даних. Аналіз п. 60 Преамбули Регламенту ЄС 2016/679 вимагає дотримання принципу прозорої та об'єктивної обробки, щоб суб'єкти даних були поінформовані про обробку персональних даних щодо них, та мету обробки. На контролера покладається обов'язок поінформувати суб'єкта про обробку та надати додаткову інформацію (наприклад, передання даних третім особам), необхідну для забезпечення прозорої та об'єктивної обробки. Якщо персональні дані відібрані безпосередньо від суб'єкта, то його має бути поінформовано, чи зобов'язаний він надавати свої персональні дані та наслідки у разі відмови від надання.

У разі надання персональних даних суб'єктом даних на контролера в момент отримання персональних даних покладається обов'язок інформувати (відповідно до ч. 1 ст. 13 Регламенту ЄС 2016/679): найменування та контактні дані контролера та його представника; згідно зі ст. 29 Керівництва Робочої групи «Про прозорість відповідно до Регламенту 2016/679», WP260 rev.01 (2018) [709]: дані мають забезпечувати легку ідентифікацію контролера та містити його контактні дані: номер телефону, електронну пошту, поштовий адрес тощо, контактні дані інспектора із захисту персональних даних; згідно зі ст. 29 Керівництва для інспекторів із захисту персональних даних (2017) [704], окремо зазначається необхідність виокремлення гарячої лінії або спеціальної контактної форми, адресованої інспектору на сайті компанії тощо. Згідно з практикою, Керівництво WP29 рекомендує організаціям сповіщати своїх співробітників про контактні дані інспектора, наприклад, у внутрішній телефонній мережі компанії.

Відповідно до ч. 1 ст. 15 Регламенту ЄС 2016/679 передбачено право суб'єкта запитувати в контролера підтвердження обробки його персональних даних та право на доступ до цих персональних даних, та отримання інформації про: (a) цілі обробки; (b) категорії відповідних персональних даних; (c) одержувачі, яким можуть бути розкриті персональні дані, зокрема одержувачі у третіх країнах або міжнародні організації; (d) за можливості, термін зберігання персональних даних, або, за відсутності такого терміну, критерії для визначення зазначеного періоду; (e) наявність можливості реалізувати право вимагати від контролера виправлення або видалення персональних даних, або обмеження їх обробки, або право заперечувати проти обробки; (f) право подання скарги до наглядового органу; (g) якщо персональні дані отримані не від суб'єкта даних, будь-яку доступну інформацію про джерело даних; (h) застосування до наданих даних процесу автоматизованого ухвалення рішення, включаючи профілювання згідно зі ст. 22(1) та (4) і, як мінімум, достовірну інформацію про відповідну логіку, а також про значущість та передбачувані наслідки зазначеної обробки для суб'єкта даних.

Відповідно до ст. 29 Керівництва із прозорості відповідно до Регламенту ЄС 2016/679, WP260 rev.01 (2018): поряд із зазначенням цілі обробки, для якої здійснюється збір персональних даних, має бути вказано правову підставу обробки за ст. 6 Регламенту. Крім того, у разі збору та обробки спеціальних або чутливих категорій персональних даних, які розкривають расове та етнічне походження, політичні погляди, релігійні або філософські погляди, членство у професійному союзі, обробки генетичних, біометричних даних, які стосуються здоров'я та сексуальної орієнтації фізичної особи, має бути посилання на відповідне положення ст. 9 Регламенту (за можливості посилання на законодавство ЄС та держав членів). Обробка персональних даних, які стосуються судимостей і правопорушень, або заходів щодо забезпечення безпеки на підставі ст. 6 Регламенту, має здійснюватися лише під контролем уповноваженого органу або, у разі, якщо обробка передбачена законодавством, то має міститься посилання на відповідні положення та підстави обробки даних контролером. Якщо персональні дані передаються третій стороні або до міжнародної організації, тоді мають міститись посилання на відповідні та належні гарантії, засоби, за допомогою яких можуть бути отримані копії даних уповноваженої особи, до якої може звертатися суб'єкт.

Так, в Австрії виник спір з цього приводу, коли суб'єкт даних звернувся до компанії, яка проводила ПЛР тести із запитом про доступ до даних щодо отримання даних про одержувачів чутливих даних через атаки та витоки даних у 2021 році. Компанія не надала інформацію про отримувачів даних через витоки, які сталися. Верховний суд Австрії (OGH Österreich, 6 Ob 242/22i) в рішенні від 24 березня 2023 року постановив, що контролер повинен був надати запитувану інформацію про порушення даних на підставі ст. 15 Регламенту ЄС 2016/679. За твердженням суду, право доступу включає будь-яку інформацію про несанкціоноване розголошення даних[694]. Це означає, що суб'єкт даних має бути поінформованим про те, що його дані були розкриті і яким чином, навіть якщо конкретний одержувач невідомий контролеру.

Наступна справа виникла стосовно розкриття даних про третіх осіб, яким передаються персональні дані користувачів. Позивач – фізична особа затребувала від відповідача – Австрійської Пошти, основного оператора почтових та логістичних послуг Австрії, розкрити дані про осіб, яким розкриваються його персональні дані (відповідно до ч. 2 ст. 15 Регламенту ЄС 2016/679). Під час судового розгляду поштовий сервіс додатково проінформував про категорії одержувачів, проте не уточнив фактичні дані осіб. Верховний суд Австрії звернувся з запитом до Суду ЄС про тлумачення ч. 2 ст. 15 Регламенту ЄС 2016/679, чи зобов'язаний контролер розкривати конкретні персональні дані одержувачів, або лише розкрити категорії, чи дозволяє стаття розкривати суб'єкту даних право знати конкретних осіб – одержувачів. Суд ЄС зазначив, що коли персональні дані розкриваються третім особам, контролери зобов'язані надати суб'єктам дані про таких одержувачів, за виключенням, якщо (a) неможливо ідентифікувати цих одержувачів, або (b) контролер може продемонструвати, що і запит суб'єкта даних є явно необґрунтованим або надмірним, і тоді контролер може вказати суб'єктам даних лише категорії відповідних отримувачів, а не розкривати фактичну особу. Суд ЄС зазначив, що розкриття даних про третіх осіб (отримувачів) суб'єктам даних може бути необхідно, щоб реалізовувати інші свої права, передбачені Регламентом ЄС 2016/679, такі як право на виправлення, видалення або право на отримання компенсації за збитки [685].

З урахуванням вище розглянутих судових рішень та аналізу законодавства ЄС, вважаємо доцільним уточнити та конкретизувати перелік інформації яку має надати контролер на запит суб'єкту персональних даних та доповнити частину 1 статті 19 Проєкту Закону України «Про захист персональних даних» від 25.10.2022 № 8153 пунктом 10 такого змісту: «інформацію про одержувачів у разі несанкціоноване розголошення даних (витоку), за виключенням, якщо неможливо їх ідентифікувати або якщо запит суб'єкта даних є явно необґрунтованим або надмірним, розкрити категорії відповідних отримувачів, а не розкриваючи фактичну особу».

Доцільно додатково звернути, увагу, вищезазначені справі є крім того свідченням, що право на доступ, виступає передумовою для ефективного здійснення право звернення до суду та третіх осіб для отримання належної компенсації, та як буде розглянуто у роботу далі, є умовою здійснення права на вправлення неточних даних у первинах даних та результатах профілюванню.

Наразі в п. 1, 2, 3, 4 ч. 2 ст. 8 Закону України «Про захист персональних даних» передбачені права, якими володіють суб'єкти персональних даних: знати джерела збирання, місцезнаходження своїх персональних даних, мету обробки, місцезнаходження або місце перебування (проживання) володільця чи розпорядника персональних даних або доручення про отримання цих даних уповноваженими особами, крім випадків, передбачених законом; отримувати інформацію про умови надання доступу до персональних даних, зокрема передачу третім особам; право на доступ до персональних даних; право отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, відповідь про те, чи обробляються персональні дані, а також отримувати зміст таких персональних даних. Вочевидь даний Закон, не відповідає умовам обробки персональних даних автоматизованими системами. Саме тому розроблений Верховною Радою Проєкт Закону України «Про захист персональних даних» від 25.10.2022 № 8153 потребує найскорішого прийняття та підписання.

Обробка персональних даних має відбуватися із дотриманням принципів обробки передбачених ст. 5 Регламенту ЄС 2016/679 серед яких: законність, справедливість та розумність; відповідність конкретних, чітких, законних цілей та не оброблятися в подальшому несумісним чином із цілями (виключення стосується подальшої обробки для архівних цілей у публічному інтересі, з метою історичних чи наукових досліджень або для статистичних цілей, які вважаються сумісними із первинною цілю; дотриманням адекватності та релевантності відповідно до мети обробки та обмеження нею (мінімізація даних)); дотриманням точності та підтриманням актуального стану, необхідності прийняття заходів для видалення неточних даних (точність даних); зберігання у

формі, яка дозволяє ідентифікувати суб'єктів даних протягом необхідного часу реалізації цілей, для яких дані обробляються, персональні дані можуть оброблятися протягом тривалого періоду виключно для архівних цілей у публічному інтересі та для цілях історичних, наукових, статистичних досліджень, за умови здійснення відповідних технічних та організаційних заходів, передбачених Регламентом ЄС 2016/679 з метою захисту прав та свобод суб'єктів даних (обмеження зберігання); дотримання способу, який забезпечує відповідну безпеку персональних даних, захист від несанкціонованої або незаконної обробки, та від випадкової втрати, знищення, пошкодження за допомогою відповідних технічних та організаційних заходів (цілісність та конфіденційність).

Сутність принципу справедливості, законності та прозорості полягає (ст. 5 (1) (a) Регламенту ЄС 2016/679) в забезпеченні поінформованості особи про обробку персональних даних та можливості суб'єкта оцінити наслідки обробки його персональної інформації та контролювати категорії даних, що використовуються. Для того, щоб обробка була законною, персональні дані повинні оброблятися на законній підставі.

Обробка відповідає законності, коли виконується одна з умов (підстав), передбачених ст. 6 Регламенту ЄС 2016/679 та ISO/IEC 27701 від 2019 р. [573], та які передбачають, що правова підстава для обробки персональних даних може містити в собі: згоду суб'єктів даних; виконання договору; дотримання юридичного зобов'язання; захист життєвих інтересів суб'єктів персональних даних; виконання завдань у суспільних інтересах; виконання законних інтересів суб'єктів персональних даних (виняток, коли перевагу над такими інтересами мають фундаментальні права та свободи суб'єкта даних, які потребують захисту персональних даних, зокрема коли є можливість належним чином встановити суб'єкта персональних даних до його здійснення). Організація повинна мати можливість продемонструвати контролюючому органу та суб'єкту даних, що вимога законності була дотримана до здійснення обробки. Організація повинна документувати цю підставу для кожної операції з обробки персональних даних

(п. 7.2.8). Законні інтереси організації можуть включати, наприклад, цілі інформаційної безпеки, які мають бути узгоджені із зобов'язаннями перед суб'єктами персональних даних щодо забезпечення конфіденційності.

Слід зазначити, що ст. 6 Закону України «Про захист персональних даних» передбачає загальні вимоги обробки персональних даних, а ч. 2 ст. 7 передбачає підстави обробки персональних даних, водночас застосування статті призначено саме до обробки окремих категорій персональних даних, які за Регламентом ЄС 2016/679 відносяться до чутливих. Аналіз законодавства ЄС та ст. 6 Закону України «Про захист персональних даних» із назвою «Загальні вимоги до обробки персональних даних» свідчить, що вона передбачає саме принципи обробки даних. Наразі ми вважаємо, що такі прогалини негативно впливають на можливість захисту прав суб'єктами даних.

Слід зазначити, що саме порушення обов'язку контролера належно повідомити про збір, обробку персональних даних суб'єктів складає значну кількість справ у практиці ЄСПЛ. У справах Perry v. The United Kingdom [402], Gaughran v. the United Kingdom [382], Catt v. The United Kingdom [377] Суд підкреслює про неналежне інформування про збір та обробку даних, що може становити порушення прав суб'єктів даних.

Збір та обробка даних має відбуватися за згодою суб'єкта даних[189, с. 93]. Робоча група зі статті 29 (WP29) провела аналіз концепції згоди відповідно до Регламенту ЄС 2016/679, переглянутого 10 квітня 2018 року (WP 259 rev.01) та розробила Керівництво зі згоди на обробку відповідно Регламенту ЄС 2016/679 [707]. На думку комісії WP29, згода є належною правовою основою лише в тому випадку, якщо суб'єкту персональних даних пропонується справжній вибір щодо використання своїх персональних даних та можливість відмовитися або відкликати власну згоду. Але WP29 також визнає певні вимоги щодо згоди, які слугують етичним стандартом або процесуальним зобов'язанням. Надання згоди на обробку може міститися в окремому документі. Причина такого розділення обумовлена потребою забезпечення суб'єкта даних права вільного вибору надання вільної згоди на обробку, яка не може ставитися в залежність від

отримання послуги або роботи. Для того, щоб згода була дійсною, вона має бути надана для «конкретної» операції з обробки даних.

До того ж, згода на обробку персональних даних не є єдиною підставою законної обробки персональних даних, у Керівництві наголошується, що компаніям не слід надмірно застосовувати згоду, а використовувати згоду як підставу для обробки даних лише тоді, коли неможливо застосувати інші підстави для законної обробки даних.

Якщо обробка має кілька цілей, згода повинна бути надана для кожної з них (у тому числі з належним повідомленням). Обробка для кількох цілей може викликати труднощі, оскільки не завжди можливо заздалегідь знати про зміну підстав обробки та може знадобитися отримання нової згоди від особи, оскільки раніше дана згода не поширювалася на нову обробку. Разом з цим, бурхливий розвиток ШІ ставить етичні та правові питання забезпечення належного захисту персональних даних та дотримання компаніями обов'язку отримувати згоду на кожну обробку даних від суб'єктів даних, яке є досить складним [883].

Слід зазначити, що одним із чинників порушення прав є низька обізнаність суб'єктів даних про обробку, мету, для якої надається згода, складність розуміння та непрозорість користувацьких угод. Залишається спірним питання про можливість дотримання засад добровільності та усвідомленості в момент надання згоди на обробку даних при поведінковій таргетованій рекламі [793, с. 15]. Користувачі в більшості випадків не усвідомлюють, що кукі-фуйли, на які вони автоматично погоджуються, збирають персональні дані [302]. У свою чергу, відмовитися від них буває технічно неможливо.

Прикладом неправильного отримання згоди та налаштувань конфіденційності можна навести рішення Суду ЄС у Справі Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände. Суд посилаючись на п. 32 Регламенту ЄС 2016/679 заявив, що згода є недійсною за допомогою попередньо зазначених прапорців, які користувач повинен зняти, щоб висловити свою відмову [375].

Разом з тим, відповідно до Регламенту ЄС 2016/679 згода на обробку залишається провідною юридичною підставою для обробки персональних даних дітей, конфіденційних даних, автоматизованого прийняття індивідуальних рішень, включаючи профілювання та передачу даних до третіх держав або міжнародних організацій.

Щодо обробки персональних даних неповнолітніх, то ст. 8, п. 58 Преамбули Регламенту ЄС 2016/679 передбачають, що згода на отримання послуг інформаційного суспільства буде законною лише у випадку, якщо вона надана безпосередньо дитиною, яка досягла 16 років. Якщо дитина ще не досягла 16 річного віку, обробка є законною в разі надання згоди особою, яка має батьківські права або схвалена нею, в цьому разі контролер, враховуючи доступні технологічні можливості, повинен зробити розумні зусилля для того, щоб переконатися у наданні згоду відповідною особою. Держави можуть передбачити нижчий вік для отримання згоди, але він не може бути нижче 13 років.

Друга ситуація стосується чутливих даних, про які зазначалося вище.

У ст. 9 Регламенту ЄС 2016/679 зазначається, що обробка чутливих або спеціальних категорій персональних даних заборонена за загальним правилом, оскільки представляє «істотні ризики для основних прав та свобод», за виключенням (ч. 2 ст. 9 Регламенту ЄС 2016/679) якщо: суб’єкт даних дав чітку згоду; обробка необхідна для цілей виконання зобов’язань та визначених прав контролера або суб’єкта даних у галузі трудового права, соціального забезпечення та соціального захисту; обробка необхідна для здійснення життєво важливих інтересів, коли суб’єкт даних не зможе дати згоду; обробка необхідна для філософських, релігійних або профспілкових цілей легітимної діяльності некомерційної організації її членів та контактних осіб; обробка персональних даних, які суб’єкт публічно розкрив; обробка необхідна для виконання або захисту законних вимог, або в межах здійснення правосуддя судами; обробка необхідна для здійснення публічного інтересу на підставі законодавства, яке має бути пропорційне переслідуваній меті, відповідати суті права на захист

персональних даних та передбачати заходи захисту фундаментальних прав та інтересів; обробка необхідна в цілях профілактичної медицини, для оцінки працездатності працівника, для діагностики медичного стану, надання медичної чи соціальної допомоги або лікування, або управління системами та послугами охорони здоров'я та соціального забезпечення; обробка необхідна через публічні інтереси в галузі громадської охорони здоров'я, захисту транскордонних загроз здоров'я або забезпечення високих стандартів якості, надійності медичного обслуговування; обробка необхідна для здійснення архівних цілей у публічному інтересі, для наукових, історичних цілей, або для статистичних цілей, які мають бути пропорційні переслідуваній меті, відповідати сутності права та захисту персональних даних і забезпечувати заходи для захисту фундаментальних прав та інтересів суб'єктів даних.

Обробка біометричних даних без належно отриманої згоди може привести до притягнення до відповідальності та накладення штрафу. Наприклад, Управління захисту даних Нідерландів наклало штраф у розмірі 725 000 євро за порушення компанією ст. 9(1) Регламенту ЄС 2016/679, через обробку біометричних даних своїх співробітників, з метою обліку відвідуваності, без наданої згоди суб'єктів даних на обробку. Компанія вимагала від співробітників сканування відбитків пальців для обліку відвідуваності. Ситуація не охоплювалася виключенням [317].

Таким чином, згода є єдиною підставою обробки, яка дійсно залежить від рішення фізичної особи. Аналогічні положення щодо необхідності отримання згоди перед обробкою чутливих даних були включені до Директиви 95/46/ЄС. Крім того, Суд ЄС у справі Bodil Lindqvist v Aklagarkammaren i Jönköping зазначив, що факт публікації чужої медичної інформації без попередньої згоди суб'єкта даних є порушенням Регламенту ЄС 2016/679 *[374]*.

Третя ситуація, коли згода на обробку залишається провідною юридичною підставою для обробки персональних даних стосується автоматизованого прийняття рішень та профілювання. Згідно із п. 71 Преамбули, ст. 22 Регламенту ЄС 2016/679 передбачено право суб'єкта даних не піддаватися рішенню, яке

засноване виключно на автоматизованій обробці персональних даних, у тому числі профілюванню, яке може викликати для нього юридичні наслідки або схожим чином суттєво впливати на нього настільки ж істотно, як наприклад, автоматична відмова від онлайн-форми заявки на кредит або працевлаштування. У цьому випадку законодавство Регламент ЄС 2016/679 захищає автономію суб'єктів даних, уповноважених дозволяти таку обробку відносно себе, оскільки автоматизована обробка може створити ризики для прав та свобод суб'єктів, адже постійне спостереження, збирання та аналіз даних можуть призвести до дискримінації та несправедливості. Приклад дискримінації та несправедливості при профілюванні наведений у ст. 5 (1) (1) Керівництва із автоматизованого прийняття індивідуального рішення та профілювання для цілей Регламенту ЄС 2016/679, коли фізичній особі відмовляють у доступі до можливостей працевлаштування, укладення договорів кредитів страхування або надають надмірно ризиковані, дорогі фінансові послуги [703].

Тож згода на обробку персональних даних, яка відповідає принципам (справедливості, законності та прозорості; збору для певної, чіткої мети; адекватність та відповідність даних поставленій меті обробки; точності та актуальності даних; способом, який дозволяє ідентифікувати суб'єкт не довше аніж потрібно; включає захист від несанкціонованого витоку та зламу) стає інструментом захисту права на недоторканність приватного життя та гарантією здійснення прав та свобод у мережі. Індивідуальна свобода також дозволяє людям відмовлятися від деяких прав, які Регламент ЄС 2016/679 має намір гарантувати. Це стосується ст. 49 Регламенту ЄС 2016/679, де за відсутності впевненості у відповідних гарантіях, включаючи обов'язкові корпоративні правила, передача персональних даних у третю країну або міжнародну організацію повинні мати місце, якщо суб'єкт даних прямо погодився на запропоновану передачу після того, як був поінформований про можливі ризики такої передачі для суб'єкта даних через відсутність рішення щодо адекватності та відповідних гарантій. Це приклад того, як згода є не лише інструментом

захисту суб'єкта даних, а й дозволяє йому йти на ризик, коли він був належним чином поінформований.

Згода на обробку залишається провідною підставою для обробки даних у ситуаціях, де існують високі ризики для прав суб’єктів даних.

Як зазначає А. Вайсман, подекуди може виникати нерівність повноважень між суб’єктами даних та контролером, що може поставити під сумнів дійсність згоди як правової підстави для обробки персональних даних[872, с. 349]. Суб’єкти не завжди дають вільну та щиру згоду, оскільки можуть перебувати під тиском, зазнати збитки через свою відмову, наприклад, коли обробка даних здійснюється органам державної влади або з метою працевлаштування [707].

Так, у преамбулі 43 Регламенту ЄС 2016/679 зазначено, що для забезпечення добровільності згоди, вона не повинна надавати допустиму правову підставу для оброблення персональних даних в окремих випадках, коли має місце явна нерівність між суб’єктом даних та контролером, особливо коли контролер є публічним органом влади і тому вільне надання згоди є маловірогідним.

Розвиток технологій автоматизованої обробки даних, IoT та зростання обсягів оброблюваних даних істотно ускладнює можливість суб’єктам даних контролювати збір, обробку, зберігання власних даних та реалізовувати свої права в інтернеті[885, с. 45]. Означене стає істотною проблемою, оскільки технології онлайн-моніторингу та відстеження стають частиною повсякденного життя.

Одна з цих проблем пов’язана з тим, що користувачі переважно ігнорують прочитання політики приватності, зокрема у сфері електронної комерції, швидко підтверджують ознайомлення з ними та погоджуються на обробку даних. За твердженням А. Макдональда та Л. Кранора, користувачам необхідно понад 244 години, щоб ознайомитися із всіма політиками приватності на платформах, які вони відвідають протягом року [662, с. 560]. До того ж, використання окремих платформ у сфері електронної комерції та отримання доступу до вмісту платформи обумовлюється попередньою згодою на обробку та підтвердженням

ознайомлення з політикою приватності, що робить обов'язковим їх прийняття, попри неясність. Тому М. Хінц піддає критиці практику складання незрозумілих політик приватності [560, с. 1050]. К. Літман-Наваро піддає критиці використання технічної, юридичної термінології та складної структури [642]. Як зазначає Т. Вайсман, практика складання заплутаних політик приватності створює «добровільне виснаження» користувачів. Науковець стверджує, що на певному етапі розвитку створення складних, довгих політик приватності було порадою юристів [872, с. 357]. Наразі така практика є хибною та неприпустимою, а в Керівництві зі згоди на обробку відповідно Регламенту ЄС 2016/679 звертається увага, що контролери не можуть розробляти занадто довгі, складні для розуміння та переповнені термінологією політики приватності [707].

З урахуванням вищевикладеного, визнаючи, що Регламент ЄС 2016/679 приділяє значну увагу згоді як підставі для обробки персональних даних, традиційна модель повідомлення та отримання згоди на обробку в умовах потужної цифровізації зазнає критики [330]. Як зазначає К. Мартін, в умовах безперервної обробки та зростання масштабів персональних даних, розвитку ШІ, традиційна модель отримання згоди з повідомленням про обробку стає неможливою для виконання, а тому потребує змін[659, с.67]. Регламент ЄС 2016/679 вимагає отримання та оформлення згоди на обробку на кожному етапі отримання нових персональних даних для їх обробки або в разі зміни мети, для якої вони були взяті. Контроль за дотриманням цієї вимоги у компанії має покладатися на інспекторів із захисту персональних даних.

Характер аналізу даних, що здійснюється системами ШІ, не припускає отримання згоди на кожному етапі нової обробки даних. З огляду на кропітливість та складність дотримання даної вимоги, висувається ідея, що фізична особа може надавати згоду або відкликати її на кожному етапі обробки персональних даних та впродовж існування відносин із постачальником послуг.

Дж. Ван Гобокен наголошує, що Регламент ЄС 2016/679 приділяє велику увагу концепції інформованої згоди, у свою чергу потужний технологічний розвиток послаблює можливість надання згоди суб'єктами даних відповідно до

його вимог, що призводить до парадоксальної ситуації [571, с. 255]. Згода є єдиною підставою для законної обробки, яка не включає критерій необхідності, що робить її застосування найбільш відповідним для алгоритмічних процесів обробки. Однак в умовах потужного розвитку технологій, отримання законної згоди для кожної мети обробки складно дотримуватися [660, с. 316].

Щоб задовольняти умовам безперервної обробки великих масивів даних, забезпечувати автоматизацію при зборі та відзиву згоди суб'єктом необхідно винайдення нової моделі отримання згоди. Висувається навіть твердження, що на підтвердження отримання згоди на обробку можуть прийматися дані з датчиків та інтелектуальних пристроїв, як-то жести, поведінкові шаблони, рухи тощо.

Будучи інструментом захисту, згода може сприйматися користувачами як перешкода користування цифровими послугами, тому порядок отримання згоди потребує адаптації до технологічних перетворень.

Дж. Карйотом висловлює підхід, підтримуваний Агентством Європейського Союзу з мережевої та інформаційної безпеки (ENISA), який має дозволити контролерам та суб'єктам даних виражати свої побажання щодо дозволених видів обробки та збереження конфіденційності оброблюваних персональних даних [592, с. 70]. Цей підхід називається: «політикою уподобань приватності». Суб'єкт даних, за допомогою формально вираженого побажання щодо конфіденційності певних категорій даних, може повідомляти контролерів про свої наміри у відношенні згоди на обробку даних, допустимих цілей обробки, дозволених одержувачів та термінів обробки тощо. Шляхом порівняння політик приватності контролера та побажань суб'єкта даних, може бути досягнута згода та домовленість про обробку даних [461, с. 47].

Відтак суб'єкт даних завантаживши додаток або оновивши програмне забезпечення в налаштуваннях приватності має зазначити підстави, мету обробки, строки обробки тощо. Такий спосіб оформлення згоди на обробку є найбільш бажаним в умовах розвитку технологій аналізу великих даних у різних сферах суспільства.

Необхідність контролю за порядком обробки персональних даних, джерелами збору, логікою алгоритмів прийняття рішень пояснюється потребою забезпечення достовірності даних, оскільки аналіз персональних даних стає основою прийняття рішень. З одного боку, контроль за даними зі сторони суб'єкта даних дозволяє забезпечувати дотримання прав людини, а з іншого, якщо суб'єкт змінює зібрані дані, то має бути передбачений контроль за діями самого суб'єкта, оскільки він може фальсифікувати дані. Означене актуалізує потребу забезпечення системи контролю, що призводить до ситуацій, коли контролери запитують перевірку документів суб'єкта даних для виявлення невідповідності та підтвердження особи. Разом з цим запит додаткових документів контролером може бути кваліфікований як порушення принципів обробки персональних даних.

Слід зазначити, що недотримання законності обробки персональних даних передбачене ст. 6 Регламенту ЄС 2016/679, в тому числі про невідповідність підстав та мети збирання, зберігання складають значну кількість порушень, які вчиняються контролерами та процесорами. На замовлення команди Д. Трампа, напередодні вибрів 2016 року, психолог А. Коган розробив психологічний тест. За допомогою тесту він збирав персональні дані для проведення академічного дослідження, про що були повідомлені користувачі. Насправді персональні дані користувачів та їх друзів підлягали збору, зберіганню, аналізу, профілюванню та переданню третій стороні, Кембрідж Аналітиці, замовнику. Про зміну мети, підстав збору, використання, зберігання та передання третім особам персональних даних користувачі не були повідомлені.

Прикладом порушення можна навести збір банком номерів телефонів для двофакторної автентифікації, тобто для більш надійного захисту користувачів та подальше передавання цих даних до маркетингового відділу для розсилання реклами на отримані номери телефонів. Подібний збір персональних даних для однієї мети та в подальшому використання для іншої називається «вторинним використанням» (secondary use). Вказані дії контролера є свідченням некоректного використання та порушують засади безпеки інформації. Тобто

користувачі надають персональні дані (номери телефонів) для використання з певною метою – забезпечення безпеки облікових записів, а зовсім не для отримання маркетингових розсилок та пропозицій про продаж.

Поряд із приватними організаціями, порушення умов збору та зберігання персональних даних відбувається з боку державних органів, про що свідчить судова практика про порушення недоторканності приватного життя. Це пов'язано з тим, що новітні технології збору та обробки персональних даних можуть ставити під загрозу здійснення особистих немайнових прав людини,.

За загальним правилом заборонена обробка генетичних даних, біометричних даних для проведення однозначної ідентифікації фізичної особи (ст. 9 Регламенту ЄС 2016/679). Через ризики нанесення матеріальної та моральної шкоди, недопущення шахрайства з персональними даними, завдання шкоди репутації або порушення професійної таємниці, обробка таких даних вимагає дотримання особливих правил для забезпечення захисту осіб від дискримінації (п. 71,75, Преамбули Регламенту ЄС 2016/679).

Відповідно до п. (f) ст. 13 Регламенту ЄС 2016/679 контролер зобов'язаний повідомити суб'єкта про намір передати його персональні дані до третьої держави чи міжнародної організації, а також наявність чи відсутність рішення Європейської Комісії про адекватність, або в разі передачі даних за умови здійснення належних гарантій (ст. 46) чи обов'язкових корпоративних правил (ст. 47), або відповідно до другого підпараграфа ст. 49(1).

Регламент передбачає обмеження на експорт персональних даних за межі ЄС. Транскордонна передача до третіх країн можлива лише за умови дотримання положень Глави V Регламенту, яка містить обмежену кількість механізмів, направлених на те, щоб передача до третіх держав не послаблювала рівень захисту персональних даних, гарантований Регламентом.

Після низки звинувачень Е. Сноудена про масове спостереження державними службами США, австрійський фахівець із захисту права на недоторканність приватного життя М. Шремс звернувся до Верховного суду Ірландії, де знаходиться європейська філія корпорації Facebook, звинувативши

керівництво корпорації в порушенні законодавства про захист персональних даних ЄС. Діюча на той момент Директива 95/46 ЄС про захист персональних даних суворо обмежувала можливості використання та збору персональних даних компаніями як GAFAM, організаціями, як Агентство національної безпеки США та передачу даних уряду від підприємств, з метою нагляду.

Позов проти Facebook став реакцією на новини про те, що американські спецслужби, зокрема Агентство національної безпеки США, можуть легко отримувати доступ до персональних даних користувачів, оскільки соціальні мережі зберігають дані користувачів на серверах у США. Таким чином, на них поширюються розпорядження про захист персональної конфіденційної інформації США, які є менш суворими, ніж у ЄС.

Справу було передано до Суду ЄС у Люксембурзі, щоб оскаржити чинність спеціальної домовленості між США та Єврокомісією від 26 липня 2000 р., яка передбачала принципи «Безпечної Гавані» (Safe Harbor) [711], які гарантували адекватний рівень захисту персональних даних громадян ЄС у разі їх експорту до США, що дозволяло корпораціям США безперешкодно обмінюватися персональними даними з державами ЄС [409]. Позов підтримав генеральний адвокат Суду ЄС Ів Бот, опублікувавши свою позицію по справі, зазначивши, що у США персональні дані громадян із держав ЄС недостатньо захищені та доступні для американських спецслужб. На погляд юриста, збір даних соцмережами порушує законодавство ЄС, яке забороняє передачу персональних даних громадян ЄС до інших держав, якщо не забезпечуються належні гарантії [727].

Результатом небезпідставних побоювань стосовно транскордонної передачі персональних даних між ЄС та США стало Рішення Суду ЄС у справі Schrems v. Data Protection Commissioner (Ireland) від 6 жовтня 2015 р. яке визнало такими, що втратили чинність принципи «Безпечної гавані» та заборонило транскордонну передачу та обмін персональних даних з державами, які мають нижчі стандарти конфіденційності, ніж в ЄС. Однією з таких держав були США. Згідно даної домовленості працювали більше 4500 компаній у США [113]. На

погляд ЄС, рішення Комісії від 26 липня 2000 р., яке передбачало принципи «Безпечної Гавані», були визнані такими, що втратили чинність через відсутність у Комісії повноважень із обмеження компетенцій національних наглядових органів. За визначенням Суду, законодавство США у сфері захисту персональних даних передбачає низькі стандарти захисту в порівняні з законодавством ЄС, тому доцільно заборонити передачу та зберігання персональних даних громадян ЄС на серверах США. Суд також зазначив, що законодавство ЄС, яке дозволяє публічній владі на загальних підставах отримувати доступ до електронних повідомлень громадян, ставить під загрозу здійснення права на повагу приватного життя.

Крім того, М. Шремс ініціював колективний позов проти Facebook, який було подано до земельного суду з цивільних справ у Відні, в якому біля 25 тисяч осіб звинуватили компанію в порушенні законодавства ЄС про захист персональних даних [787]. Позивачі вимагали від Facebook символічну компенсацію – по 500 євро кожній особі. Суд відхилив позов, після чого М. Шремс подав апеляцію.

За висловленням депутатів ЄС, Єврокомісія насміхалася над громадянами ЄС, адже за останні 15 років дії «Безпечної Гавані», мільярди персональних даних громадян ЄС були передані в США із порушенням основоположних прав [58].

У зв’язку з невідповідністю принципів «Безпечної Гавані» законодавству ЄС, на продовження позиції Суду ЄС у даній справі, у 2017 році Європарламент звернувся до Суду ЄС для отримання відповіді про відповідність домовленості між ЄС і Канадою про передачу й обробку даних пасажирів Passenger Name Record, вимогам ст. 7 та 8 Хартії ЄС про основні права, з урахуванням захисту персональних даних. Дана Угода дозволяла систематичну та безперервну передачу даних пасажирів (дані пасажирів, що зберігаються авіаперевізниками в їх системах бронювання та реєстрації) канадському органу з метою використання та зберігання цих даних, подальше передання органам держав, які не є членами ЄС з метою боротьби з тероризмом та іншими формами

транснаціональної злочинності. Суд ЄС висловив позицію від 26 липня 2017 р. № 1/15, що запропонована Угода про передачу персональних даних пасажирів є несумісною з правом на захист приватного життя та стандартами захисту персональних даних, визнаними в ЄС [724].

На заміну «Безпечній Гавані», яке втратило чинність, ЄС та США уклали угоду Privacy Shield, затверджену Рішенням Комісії ЄС 2016/1250 про адекватність захисту персональних даних при передачі з ЄС до США. Відповідно до угоди, на компанії США покладався обов'язок суворо ставитися до захисту персональних даних, проводити більш надійний моніторинг та забезпечення виконання зобов'язань у тісній співпраці з наглядовими органами із захисту персональних даних ЄС. GAFAM повинні були прийняти типові положення для кожного випадку передачі персональних даних з ЄС до США, дотримуючись вимог ЄС [710]. Тож у зв'язку з рішення Суду ЄС від 6 жовтня 2015 р., компанії були змушені укладати типові договірні положення з трансферу персональних даних для продовження їх передачі до США.

Проте, у зв'язку з новою скаргою М. Шремса на Facebook, Суд ЄС від 16 липня 2020 року прийняв рішення, що угода Privacy Shield, яка використовується технологічними компаніями, банками, фінансовими установами для передачі персональних даних з ЄС до США, не захищає персональні дані та приватне життя громадян ЄС. З огляду на думку М. Шремса, що стандартні положення контракту з трансферу даних – standard contractual clauses SCC не гарантують належний захист персональних даних та приватного життя резидентів ЄС при їх передачі на сервери за межі ЄС, зокрема в роботі таких компаній як Facebook, Суд ЄС визнав недійним Рішення Комісії ЄС 2016/1250 про затвердження адекватності захисту персональних даних в угоді Privacy Shield [379]. Суд визнав, що вимоги національної безпеки США, спільних інтересів та правозастосування порушують основні права осіб, чиї персональні дані передаються в США. За оцінкою Комісії ЄС 2016/1250, обмеження в належному захисті персональних даних, які випливають із внутрішнього законодавства США, не відповідають вимогам, по суті передбаченим законодавством ЄС. Суд

визнав, що положення окремих державних програм спостереження США не накладають обмежень на повноваження, які вони надають для реалізації цих програм, або на наявність правових гарантій для осіб, не громадян США.

Ці положення хоча й передбачають вимоги, які державні органи США мають дотримуватися при реалізації програм спостереження, водночас ці положення не надають суб'єктам даних права на звернення до суду для оскарження дій держаних органів США. За твердженням Суду ЄС, обмеження із захисту персональних даних, що випливають із національного законодавства США про можливість доступу до цих даних органам влади США, в даному рішенні Європейської Комісії не передбачені так, щоб вони були рівноцінні вимогам законодавства ЄС у частині принципу пропорційності, оскільки застосування програм стеження на основі цих положень не є чітко обмеженими суворою необхідністю.

Суд ЄС зазначив, що попри Рішення Комісії ЄС 2016/1250, механізм омбудсмена, передбачений у цьому рішенні, не містить підстав суб'єктам даних для певних дій та не надає гарантій, еквівалентних законам ЄС, та не передбачає гарантій незалежності омбудсмена та повноважень прийняття рішень, які б покладали зобов'язання на державні органи. У зв'язку з визнанням Судом ЄС Рішення Комісії ЄС 2016/1250 стандартів захисту персональних даних неадекватними до вимог законодавства ЄС, компанії зі США, які займаються збором та обробкою персональних даних на території ЄС, мають приймати стандартні договірні положення захисту персональних даних, (являють собою попередньо схвалені контракти, які забезпечують правове підґрунтя для передачі даних між ЄС та США) або використовувати обов'язкові корпоративні правила (по суті внутрішні правила для передачі персональних даних на територію США) відповідно до вимог Регламенту ЄС 2016/679.

З урахуванням викладеного, можна стверджувати, що Директива 95/46 ЄС та Регламент 2016/679, без сумніву, стали стандартом для захисту прав фізичних осіб у всьому світі та значна кількість держав обрали шлях односторонньої регуляторної глобалізації, а визнання Судом ЄС «Безпечної Гавані» та «Щита

Приватності» такими, що не відповідають стандартам захисту прав суб'єктів даних – наслідком «брюссельського ефекту» для технологічних компаній [347]. Крім того, обмеження на передачу персональних даних в юрисдикції держав, які не забезпечують законний збір, обробку персональних даних та належні гарантії прав недоторканності приватного життя поряд із законною згодою суб'єкта на обробку даних є гарантією недоторканності приватного життя та засобом правового захисту персональних даних фізичних осіб у мережі.

Наступне право, концептуалізація якого є результатом прийняття Регламенту 2016/679 – право суб'єктів на видалення персональних даних або «право на забуття». Право на забуття обмовлено властивістю інтернету до збереження безмежної кількості інформації, створюючи передумови порушення недоторканності приватного життя. За таких умов право на забуття покликано надати певний контроль суб'єктам за обробкою даних в інтернеті.

Дане право покликано балансувати між правом на доступ до інформації, правом на вираження думки та правом на недоторканність приватного життя та захистом персональних даних, що закріплені у ст. 7-8 Хартії ЄС про основні права [426]. Сформульоване в Регламенті 2016/679 право на забуття є результатом кропіткої роботи Європейської комісії, Європейської Ради та Європейського Парламенту.

Право бути забутим існувало в певній обмеженій формі до потужного розвитку цифровізації та прийняття Регламенту 2016/679, водночас його закріплення в законодавстві стало важливою віхою розвитку цифрових прав. Право на забуття не застосовується до випадків, коли обробка персональних даних необхідна для: 1) здійснення права на свободу вираження думки та свободу інформації; 2) дотримання виконання правових вимог законодавства ЄС, держав членів, виконання задач в інтересах суспільства, при виконанні офіційних повноважень контролера; 3) забезпечення суспільних інтересів у галузі охорони здоров'я; 4) проведення архівування, наукових та історичних досліджень; 5) реалізації судочинства.

Як зазначає О.М. Калітенко [71, с. 84], баталії з приводу законодавчого закріплення даної норми обумовлено тим, що право бути забутим знаходиться на межі двох особистих немайнових прав: права на інформацію, яке проявляється в безперешкодному доступі до неї, права на вираження власної думки (ст. 19 ЗДПЛ) та, з іншого боку, права фізичної особи на приватність, повагу до свого приватного та сімейного життя, та захист персональних даних (ст. 7, 8 Хартії ЄС про основні права, ст.12 ЗДПЛ) [65].

Одним із резонансних випадків судової практики щодо здійснення права на видалення стала справа Google проти Маріо Костехі Гонсалеса, розглянута Судом ЄС у 2014 році [386]. У 2010 році громадянин Іспанії К. Гонсалес подав до Іспанського агентства з захисту персональних даних скаргу на компанію Google Spain, вказуючи на порушення прав, у результаті того, що під час пошуку його імені в Google видаються посилання на публікації про несплату ним податків у 1998 році.

Верховний суд Іспанії звернувся із запитом до Суду ЄС за попередньою постановою. Відповідно позиції Суду, фундаментальні права на повагу приватного життя та захист персональних даних переважали не лише економічний інтерес оператора пошукової системи, а й суспільний інтерес в отриманні доступу до інформації, яка носить персональний характер. За твердженням Суду, в окремих випадках обмеження фундаментальних прав допускається в разі публічної ролі суб'єкта та інтересу суспільства.

Тож рішення у справі Google проти К. Гонсалес викликало дискусію навіть серед прибічників права. Адже постало питання щодо кваліфікації операторів пошукових систем як контролерів, операторів персональних даних, фактично покладаючи на них обов'язки із проведення видалення пошукових посилань та фільтрування результатів таких пошуків [736, с. 325]. Про дискусійний характер рішення свідчить і те, що генеральний адвокат Суду ЄС Н. Яскинен не погодився з положенням про можливість обробки персональних даних операторами пошукових систем [726].

Рішення у справі К. Гонсалеса вплинуло на закріплення можливості здійснення права на забуття в інтернеті. Адже Суд визнав посилання в системі пошуку більш значущим втручанням у приватне життя, здатним порушити особисті немайнові права особи, аніж публікацію. Суд виходив із того, що в умовах інформаційного суспільства посилання на публікацію забезпечує легкий доступ до неї значному колу осіб. Водночас постає слушне питання, наскільки вірогідно досягти баланс між публічними та приватними інтересами, між правом на вільний доступ до інформації та здійсненням права на приватність шляхом видалення посилання на публікацію в пошуковій системі.

У цьому сенсі цікаве твердження Л. Флоріді про те, що в умовах цифровізації видалення посилання в пошуковій системі рівнозначно знищенню книги в минулому. Наразі відсутність інформації в інтернеті прирівнюється до відсутності посилання в пошуковій системі, а видалене посилання перетворює публікацію в майже неіснуючу [519, с. 3].

Надалі у справі Гурбейн проти Бельгії, ЄСПЛ підтвердив позицію, висунуту у справі Костехи Гонсалес. Особа засуджена за вчинення ДТП із двома загиблими у 2000 році та реабілітована у 2006 році вимагала видалення з пошукової системи посилання на архівну публікацію бельгійської газети за 1994 рік [368]. ЄСПЛ у своєму рішенні прийшов до висновків про те, що: законодавство Бельгії визнає право бути забутим як невід'ємною складовою права на недоторканність приватного життя, що особа будучи водієм, не є публічною особою та діяльність не являє суспільного інтересу; існування матеріалу в електронному вигляді може більше впливати на приватне життя, аніж ці ж матеріали у друкованих ЗМІ; для засудженої особи існування старих архівних матеріалів в електронній формі про вчинене правопорушення не повинно ставати стигматизацією в майбутньому; баланс між правом на вираженням поглядів та здійснення права бути забутим можливо досягти шляхом анонімізації прізвища водія в архівних новинах, без необхідності видалення самого друкованого матеріалу.

У справі 28 червня 2018 р. ЄСПЛ відхилив заяву про порушення права на недоторканність приватного життя за ст. 8 ЄКПЛ та вимогу про право на забуття у зв'язку з визнанням особи винною у вбивстві. Справа стосувалася двох громадян Німеччини, М.Л. та В.В., засуджених до довічного ув'язнення за вбивство популярного німецького актора, вчинене у 1991 році. У 2000 році вони безуспішно намагалися домогтися поновлення справи, про що повідомили місцеві ЗМІ. У 2007 році заявники звернулися до суду з вимогою анонімізувати опубліковані новини. Федеральний суд Німеччини відхилив позов, спираючись на суспільний інтерес. У подальшому ЄСПЛ, підтримав рішення Федерального суду Німеччини, посилаючись на те, що в даній ситуації право на доступ до даних переважає право на недоторканність приватного життя [396].

Визнаючи, що вчинки, стосунки або факти про особу мають розглядатися як сфера недоторканності її приватного життя, водночас ця сфера може варіюватися залежно від конкретного змісту норм, традицій та культури держави.

О. Полічіано звертає увагу про неможливість застосування права на видалення по відношенню до персональних даних у реєстрі компаній. Означена позиція висловлена в постанові Суду ЄС у справі Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni [376]. Якщо у справі Google Spain право на недоторканність приватного життя та захист даних вступає у протиріччя з необхідністю забезпечити свободу вираження думки та права на доступ до інформації та свободи ведення підприємницької діяльності у зв'язку з діяльністю цифрових платформ, то у справі Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni спір точиться між правом на недоторканність приватного життя та забезпеченням прозорості ділових відносин з метою сприяння розвитку внутрішнього ринку [743, с. 659].

Б. Кастерс піддає критиці право на видалення персональних даних, передбачене Регламентом ЄС 2016/679, через передбачені виключення та обмеженість його здійснення, оскільки ст. 17 Регламенту ЄС 2016/679 істотно врівноважує інтереси контролерів даних та суб'єктів даних. На погляд науковця,

право на видалення не є основним правом, по-перше, тому що воно міститься у вторинному, а не в основному законодавстві, і, по-друге, тому що воно не є абсолютним правом та передбачає виключення.

М. Фазліоглу дотримується аналогічної позиції, що право на видалення носить обмежений характер та контролери не завжди зобов'язані співпрацювати із запитами суб'єктів даних [511, с. 149].

З огляду на зазначене, поряд із законодавчим закріпленням права на видалення, у доктрині висувається ідея про існування права почати все з чистого цифрового аркушу, яке покликано дозволити особам дійсно розпочати абсолютно нову цифрову ідентичність[447, с. 4]. Оскільки алгоритми збирання та профілювання великих даних є механізмами, які з часом автоматично посилюються, про що зазначає винахідник Google Р. Курцвейл, то навіть незначні відхилення, неправильні або неповні дані можуть в подальшому призвести до посилення неточностей у висновках та профілях. Наприклад, спостереження правоохоронними органами в більшій мірі будучи зосередженими у неблагополучних районах міст, може призвести до упередженого та суб'єктивного заповнення баз даних та профілювання мешканців цих районів, навіть за відсутності їх девіантної поведінки. Відомі ситуації, коли випадкові дані, винайдені в інтернеті через роки, завдавали значної шкоди репутації особи [750].

Право почати все з чистого цифрового аркуша можна порівняти з, ситуацією надання можливості розпочати життя з чистого аркуша особі після відбування покарання. Про негативні наслідки профілювання в діяльності правоохоронних органів, звертає увагу Human Rights Watch [572].

Розробка права на чистий цифровий аркуш тісно пов'язана із викликами, які несе аналіз великих даних та профілювання. Аналіз даних у залежності від поставленої мети, може проводитися для опису або прогнозування [450, с. 15]. Аналіз даних, проведений алгоритмом, надає можливість визначити закономірності в поведінці осіб та обґрунтувати схильності до вчинення певних дій [882, с. 210]. Державні органи можуть використовувати алгоритми для оцінки

повторного вчинення правопорушення особами із певним психологічним профілем. Приватні компанії та державні установи використовують аналіз персональних даних для: оцінки кредитоспроможності клієнтів; покращення якості послуг; проведення дослідження; управління персоналом; виявлення злочинної діяльності та шахрайства [669, с. 40]; відправлення маркетингових повідомлень.

Слід окремо зупинитися на тому, що розуміється під «профілюванням». Профілювання відноситься до виду автоматизованої обробки персональних даних (п 4. ст. 4 Регламенту ЄС 2016/679) – будь-яка форма автоматичної обробки персональних даних, яка полягає у використанні персональних даних для оцінки певних особистих якостей фізичної особи, зокрема, для аналізу чи передбачення аспектів ефективності в роботі, економічного статусу, здоров'я, особистих переваг, інтересів, надійності, поведінки, місцезнаходження чи переміщення, які породжують правові наслідки, що стосуються суб'єкта даних чи істотно впливають на нього. Регламент ЄС 2016/679 визначає проведення профілювання, якщо вчинено: збір та аналіз персональних даних у великих масштабах з використанням алгоритмів, штучного інтелекту або машинного навчання; встановлення асоціацій для побудови зв'язків між різними патернами поведінки та атрибутами; створення профілів, які застосовуються по відношенню до фізичних осіб; прогнозування поведінки окремих фізичних осіб на підставі їх профілів.

Профілювання передбачає аналіз персональних даних для класифікації осіб на певні групи, виявлення кореляцій між різними моделями поведінки та подальше створення профілів осіб. Наслідком такого аналізу є нові дані про фізичну особу, які стають частиною профілю.

За твердженням Р. Кларка, профілювання використовується державними органами для конструювання стереотипів поведінки та профілів, таких як: терористи, торгівці наркотичними речовинами, особи схильні до вчинення насильницьких злочинів, які ухиляються від сплати податків, шахраї у сфері соціального забезпечення та страхування, підлітки схильні до вчинення

самогубства тощо [434]. Так, наприклад, Міністерство соціальної політики України використовує автоматизовану систему аналізу великих даних для виявлення осіб, які отримують незаконно соціальну допомогу [283]. Профілювання використовується корпораціями для виявлення споживачів, які можуть бути сприйнятливими до реклами товарів, послуг, а також претендентів на вакантні посади.

Л.А. Байгрейв визначає профілювання як об'єднання низки характеристик (профілю) про особу або організацію із подальшим ставленням до особи відповідно до цих характеристик [451, с. 50].

Сфера застосування цифрового профілювання розширюється, та якщо від початку застосовувався переважно у сфері маркетингу, то поступово почав застосовуватися для забезпечення безпеки, в державному управлінні, здійсненні судочинства, наданні державних послуг та працевлаштування. Профілювання може використовуватися для захисту організацій та компаній від внутрішніх ризиків: виявлення підозрілих співробітників, поведінка яких в мережі обробляється та аналізується; працевлаштування та відстеження ефективності виконання трудових обов'язків та перевірки відповідності займаній посаді, заохочення тощо.

За визначенням М. Хільдебрандта, персональні дані користувачів підлягають профілюванню з метою: визначення уподобань для надання персоналізованих товарів та послуг, через загрозу інформаційної безпеки, шахрайства та відмивання доходів, отриманих злочинним шляхом [557, с. 175]. Науковець звертає увага на такі аспекти профілювання як процес виявлення патернів різних даних, які можуть використовуватися для ідентифікації особи та застосування профілів (низки корелюючих даних) для індивідуалізації суб'єкта або для його ідентифікації як учасника спільноти[558, с. 55].

В означених підходах акцентується увага на таких властивостях профілювання як: пошук інформації за визначеними критеріями, зв'язок даної інформації із конкретною особою, використання інформації для ідентифікації особи або для певного поводження із особою.

Одним із негативних наслідків профілювання є неупередженість результатів, про яку мова піде нижче. З погляду Т. Колдерса та Б. Кастерса, оскільки алгоритми профілювання та прогнозування ризику можуть застосовуватися для отримання профілів осіб, потенційно здатних вчинити правопорушення, з баз даних правоохоронних органів результати будуть свідчити, що правоохоронні органи зосередили свою діяльності та спостереження за цими районами, в результаті дані від початку будуть містити упередженості [448, с. 10]. Таким чином мешканці навіть без ознак девіантної поведінки будуть під пильним наглядом правоохоронних органів. Також посилення нагляду може призводити до стигматизації цих районів, зниження вартості нерухомості та ускладнення можливості позбавитися від профілів та стереотипів, які стануть перешкодою в подальшому, щоб змінити район проживання. Такі результати профілювання можуть залишитися з особою протягом життя.

Прикладом використання профілювання є – редлайнінг, під яким розуміється відмова державними органами, суб'єктами підприємницької діяльності у продажі товарів, наданні послуг або підвищення їх вартості в певних районах міста, відзначених червою лінією [569]. Редлайнінг наразі заборонений законодавством США, існував внаслідок збільшення демографічної концентрації людей зі схожим соціальним статусом, умовами працевлаштування та національної приналежності, в певному районі проживання [344, с. 20].

З урахуванням зазначеного, що внаслідок цифрового профілювання створюються нові дані, які не є ідентичними тим, які були надані суб'єктом даних, а метод профілювання створює значні ризики для прав та свобод людини, коли людина може потрапляти в певні категорії, навіть про це не знаючи. Тож профілювання може призводити до обмеження прав на доступ до певних товарів та послуг, створюючи дискримінацію. Відтак профілювання створює не лише можливості для управління даними та розвитку цифрової економіки, а й підвищує ризики втручання у сферу приватного життя. Подібні методи цифрового профілювання та соціального рейтингу використовуються в КНР.

Уявляється, що огляд наслідків обробки великих даних є досить переконливим у необхідності розробки прав на цифровий аркуш, крім того прибічники даного права вважають, що воно має охоплювати право на захист суб'єктів у разі профілювання компаніями та державними органами при прогнозуванні майбутньої поведінки та оцінки вірогідності вчинення повторного правопорушення та недопущення стигматизації раніше засуджених осіб [225, с. 45]. Водночас на погляд прибічників права на цифровий аркуш, воно має охоплювати набагато ширше коло питань, які не можуть бути вирішені за допомогою антидискримінаційного законодавства.

Цікавою в цьому сенсі є практика ЄСПЛ щодо зберігання особистої інформації в базах даних правоохоронних органів, яка формувалася з огляду на потребу врахування тяжкості злочину, суспільного інтересу та права на доступ до інформації про особу та вчинений злочин, при прийнятті рішення про можливість видалення таких даних із інформаційних систем. У справах B.B. v. France [373] та Gardel v. France [381] дискусійним було питання, чи слід вважати включення в національну систему бази даних інформації про осіб, які вчинили злочини проти статевої свободи та недоторканості, порушенням ст. 8 Конвенції Ради Європи 1981 року «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Відповідно до обставин справи дані мали зберігатися впродовж 20-30 років залежно від тяжкості злочину. ЄСПЛ взяв до уваги тяжкість злочинів та інтерес суспільства в існуванні таких баз даних та прийшов до висновку, що в даних справах не відбулося порушення ст. 8, з огляду на існування процедури пред'явлення вимоги про вилучення інформації з бази даних. У справі M.M. v. the United Kingdom заявниця скаржилася на зберігання та розкриття попередження поліції про викрадення дитини, яке не було вилучене з матеріалів її справи, яка зберігалася в поліції [397]. У справі Dalea v. France [378] заявник скаржився, що зберігання інформації про нього в інформаційній системі держав Шенгенської угоди обмежувало його в'їзд до Шенгенської зони та ставало причиною у відмовах у видачі віз з особистою та професійною метою. Його скарга була визнана неприйнятною за ст. 8 та ЄСПЛ зазначив, що заявник

міг оскаржити пропорційність застосування цих заходів у різних національних органах.

Цікавим у цьому аспекті є факт, що у Великобританії зібрана досить масштабна база даних ДНК осіб, що були заарештовані за підозрюю у вчиненні злочинів. На відміну від Шотландії, де відомості вилучаються з бази, якщо особа виправдана, в Англії та Уельсі дані можуть зберігатися впродовж багатьох років. Незважаючи на те, що правозахисні організації висловлюють побоювання щодо порушення прав через довготривале зберігання даних, правоохоронні органи прагнуть розширити цю базу за рахунок включення даних про неповнолітніх, які вчинили правопорушення та інших категорій громадян та вбачають порушення прав людини [638, с. 485].

З огляду на зростання потреби у транскордонному обміні даними, актуальність питань, пов'язаних зі зберіганням та обробкою даних у національних та європейських системах даних у практиці національних судів та ЄСПЛ буде зростати, з огляду на поширення таких баз даних. Лише на європейському рівні слід назвати такі бази: ШІС (Шенгенська інформаційна система), МІС (Митна інформаційна система) та ВІС (Візова інформаційна система). Крім того, відповідно до даних Європейського наглядового органу захисту інформації, за останні десять років відзначається зростання міжнародного співробітництва правоохоронних органів та судів у боротьбі з терористичною діяльністю та іншими формами міжнародної організованої злочинності, що забезпечується обміном інформацією між державами.

Слід констатувати, що здійснення права суб'єкта заперечувати проти подальшої обробки даних або право на чистий цифровий аркуш та обов'язок оператора даних видаляти інформацію негайно після того, як вона перестає бути необхідною, для цілей опрацювання відбувається із врахуванням права на доступ до інформації, інтересу суспільства в доступі до цих даних [302].

Із профілюванням тісно пов'язане право на виправлення неточних даних, зібраних в електронних базах даних, передбачене ст. 16 Регламенту ЄС 2016/679. Про потребу закріплення права на виправлення неточних персональних даних,

зібраних в електронних базах даних, наголошувалося ще в Резолюції Ради Європи Про захист конфіденційності фізичних осіб по відношенню електронних баз даних у недержаному секторі від 26.09.1973 [753].

Регламент ЄС 2016/679 наділяє суб'єктів даних правом вимагати від контролера без невиправданих зволікань, виправити неточні персональні данні щодо нього. З урахуванням мети обробки уточнення даних суб'єкт має право на внесення доповнень до неповних персональних даних шляхом подачі заяви (ст. 16 Регламенту ЄС 2016/679). Суб'єкт має право надавати додаткові персональні дані для уточнення. У залежності від мети обробки контролер може прийняти або відхилити додані персональні дані. Внесення змін провадиться безоплатно (п. 59 Преамбули Регламенту ЄС 2016/679). Регламент не містить визначення, що має розумітися під неточними персональними даними. Разом з цим Суд ЄС у справі Новака проти Комісара із захисту персональних даних [403] зазначив, що відповіді особи під час здачі іспиту визнаються персональними даними, але право на уточнення не може бути застосовано до випадків виправлення неправильних відповідей на іспиті. Правом на уточнення особа може скористатися в разі доповнення або виправлення неповної інформації у випадку профілювання, коли компанія складає профілі співробітників або користувачів з різних підстав (продуктивність праці, маркетинг тощо). Тобто ситуація, коли компанія здійснює профілювання, застосовує автоматизовану обробку персональних даних для прийняття рішень, аналізу або прогнозування особистих переваг, поведінки чи установок (згідно зі ст. п. 24 Преамбули).

Припускається, що особа, яка піддається профілюванню, може скористатися своїм правом на доступ до даних за ст. 15 Регламенту ЄС 2016/679, щоб дізнатися, які дані щодо неї були використані для складання профілю та зміст профілю, а в разі виявлення невідповідності первинних даних, оскаржити неточність профілю та коректність використання персональних даних. Відповідно до Керівництва із автоматизованого прийняття індивідуального рішення та профілювання, право на виправлення наділяє суб'єкта можливістю виправити або внести зміни в неточності у профілюванні [703], у разі включення

особи до категорії, яка не відповідає її здібностям або категорію, яка не відповідає стану здоров'я.

Чинне законодавство не передбачає право на виправлення, а така норма пропонується у ст. 20 у Проєкті Закону Україні «Про захист персональних даних» від 25.10.2022 № 8153 [140]. Разом з тим, ми вважаємо доцільним доповнити статтю 20 Проєкту Закону України «Про захист персональних даних» частиною 4 такого змісту: «право суб'єкта персональних даних на виправлення персональних даних передбачає право внесення виправлень в результати неточного профілювання».

Окрему увагу слід приділити праву на перенесення персональних даних, яке передбачає створення можливості для суб'єкта персональних даних запросити в контролера персональні дані, які він обробляє, отримати їх у доступній формі та просити передати такі дані іншому оператору (ст. 20 Регламенту). Право на перенесення персональних даних отримало широке висвітлення в дослідницькій літературі ще до набрання чинності Регламенту ЄС [554, с. 200]. Проєкт Закону України «Про захист персональних даних» передбачає у ст. 23 аналогічне за змістом право на мобільність персональних даних.

За змістом п. 68 Преамбули Регламенту право на перенесення, відповідно до Керівництва з права на перенесення даних [719], покликано надати «користувачу контроль та розширення прав і можливостей», адже це право спрямоване на посилення користувацького контролю за власними даними. Перенесення даних дає змогу користувачам отримувати копії своїх персональних даних і, в певному сенсі, може розглядатися як право на доступ до своїх персональних даних (стаття 15 Регламенту). Також це може допомагати користувачам без втрати своїх даних звертатися до постачальників більш якісних послуг.

Право на перенесення персональних даних за змістом Регламенту ЄС 2016/679 може бути розділене на два окремі права: право на отримання персональних даних у «структурованому, повсюдно використовуваному та

машино читабельному форматі», та право на передачу отриманих персональних даних без зміни до іншого оператора. Право на перенесення можна застосовувати при дотриманні таких двох умов: дані були отримані контролером на підставі згоди або на умовах, передбачених договором; дані оброблені із застосуванням автоматизованих систем, що виключає використання паперової документації (Керівництво).

У Керівництві зазначено, що право на перенесення застосовується відносно даних: які отримані в результаті активних дій користувача (записи, історія відвідувань, пошукова активність, місцезнаходження тощо), які мають розглядатися як дані, надані користувачем; які добровільно залишені користувачем, шляхом прямих дій; які були згенеровані в результаті використання додатку або послуги. Як зазначають деякі критики, офіційне тлумачення розширює межі права на перенесення даних за межі тексту самої статті та законодавчого сенсу.

Право не перенесення поширюється лише на персональні дані та виключає можливість перенесення анонімних даних або даних, які не стосуються користувача (Керівництво).

Враховуючи викладене, аналіз Регламенту та Керівництва дозволяє стверджувати, що ст. 23 Проєкту Закону «Про захист персональних даних» передбачає право контролера вимагати компенсацію від суб'єкта персональних даних, якщо здійснення цього права покладає надмірний тягар на контролера, слід визнати сумнівною. Оскільки сама ідея здійснення цього права стосується ситуації обробки, яка відбувалася із застосуванням автоматизованих засобів, а з тим не передбачає надмірних зусиль з боку контролера.

В умовах автоматизації особливого значення набуває право не піддаватися рішенню, яке засноване виключно на автоматизованій обробці персональних даних, передбачене ст. 22 Регламент ЄС 2016/679. У тому числі не піддаватися профілюванню, яке може викликати для суб'єкта юридичні наслідки або схожим чином впливати на нього настільки ж істотно, як наприклад, автоматична

відмова в онлайн-формі заявки на отримання кредиту або участь у конкурсі на заміщення вакантних посад онлайн без участі фізичної особи.

Рішення, які донедавна приймалися фізичними особами як право на отримання соціальної виплати, банківського кредиту, укладення договору страхування наразі автоматизуються. Оскільки прийняття юридично значущих рішень алгоритмами на підставі аналізу великих даних можуть бути помилковими та спричиняти наслідки для суб'єктів даних, на компанії покладаються обов'язки дотримання умов використання автоматизованих систем та отримання згоди суб'єкта даних для такої обробки.

Правові проблеми використання систем штучного інтелекту, зокрема питання меж прийняття юридично значущих рішень із використанням автоматизованих систем або делегування прийняття рішень із використанням систем штучного інтелекту, значний час є предметом дискусії в юриспруденції, психології, соціології, у дослідженнях концепцій філософії, техніки Б. Латура [617, с. 45]. Питання делегування повноважень агентам та автоматизованим системам детально буде розглянуто у підрозділі 3.4. «Основні положення про дієздатність фізичної особи у відносинах у мереіж «Інтернет»».

Прийняття юридично значущих рішень може передбачати різний ступінь автоматизації процесу прийняття рішення [316, с. 55]. Залежно від ступеня та якості втручання людини у процес прийняття рішення можна розрізняти системи: повністю автоматизованого прийняття рішень, які не залежать від участі людини та частково автоматизовані із остаточним прийняттям рішення людиною. У зв'язку з ризиком порушення прав людини, Регламент ЄС 2016/679 вимагає від суб'єктів господарювання не приймати рішення стосовно фізичних осіб, які засновані виключно на автоматизованій обробці персональних даних, тобто прийняття рішення системою ШІ. Для того, щоб запобігти такій практиці на контролера даних, який здійснює профілювання, покладено обов'язок використовувати автоматизовану процедуру спільно з остаточним прийняттям рішення людиною. Контролер зобов'язаний вжити заходи для запобігання прийняття рішень, заснованих на даних про расу, етнічне походження, політичні

переконання, релігію, членство у профспілковій організації, генетичних схильностях, стану здоров'я або сексуальної орієнтації (п. 71 Преамбули). Слід зазначити, що дане положення Преамбули передбачає не виключення обробки спеціальних категорій персональних даних, а саме недопущення прийняття рішення на основі таких даних, означене обумовлено технологічною специфікою обробки великих масивів даних, які не передбачають можливість виключення категорій даних із усього масиву інформації, водночас дозволяють не брати до уваги певні дані на етапі їх аналізу та прийняття рішення.

Відповідно до п. 71. Преамбули Регламент ЄС 2016/679 допускає прийняття рішень, заснованих на автоматизованій обробці, включаючи профілювання, якщо це безпосередньо дозволено законодавством ЄС або держав-членів, суб'єктом якого є контролер, включаючи моніторинг шахрайства та ухилення від податків, запобіжних заходів, які провадяться відповідно до законодавства для забезпечення безпеки та надійності послуг, що надаються контролером, або необхідно для укладання чи виконання договору між суб'єктом даних і контролером, або коли суб'єктом даних було надано пряму згоду.

Оскільки наразі застосування повністю автоматизованого прийняття рішення є виключенням, значні побоювання викликає застосування автоматизованих систем озброєння. Р. Сюарт та Дж. Хіндс наводять приклад використання роботизованих систем, віддаленої біометричної ідентифікації з метою виявлення воєнної цілі [801]. Міжнародний Комітет Червоного Хреста зазначає, що повністю автономні системи, поряд із певними перевагами, як здатність заміняти військових [575], несуть в собі загрозу фундаментальних етичних проблеми людства, адже ставлять питання, наскільки етично дозволяти програмі, роботизованій техніці позбавляти людину життя [576]. Тому рекомендується державам заборонити використання непередбачуваних автономних систем озброєння, зокрема через їх невибіркову дію, за виключенням дотримання певних вимог.

Аналіз великих даних для розвитку машинного навчання ставить питання прозорості застосування систем автоматизованого прийняття рішень та

контролю над ним суб'єктами персональних даних, оскільки випадки прийняття рішень виключно системами, без участі людини залишаються поодинокими. Під час застосування технології автоматизованого прийняття рішень мають бути визначені критерії, задані користувачем, який має прийняти остаточне рішення. Наприклад, програма для пошуку фахівців на зайняття вакантних посад обирає кандидатів за певними критеріями: вік, досвід роботи тощо. Остаточне рішення, оцінку навиків претендентів, що не може відображатися в резюме, приймає фізична особа. Відтак, коли фізична особа використовує лише інформацію, надану системою, не беручи до уваги додаткові чинники, рішення є виключно автоматизованим.

Оскільки повна автоматизація може бути небажаною під час прийняття юридично значущих рішень, зазвичай автоматизуються лише окремі частини складного процесу ухвалення [463, с. 85]. Крім того, з антропоцентричного підходу випливає необхідність участі фізичної особи при прийнятті юридично значущих рішень, що обумовлено уявленням, що саме право конструює та регулює відносини між суб'єктами – людьми.

З метою забезпечення прав людини під час автоматизованого профілювання та прийняття рішень, які спричиняють юридично значущі наслідки ст. 22 Регламенту ЄС 2016/679 та ст. 11 Директиви про захист даних у кримінальних провадженнях 2016/680 [716], передбачає положення, покликані захистити фізичних осіб та суворо передбачає умови, при яких дозволяється використання системи алгоритмів при прийнятті рішень. Компанії мають право використовувати системи алгоритмів при прийнятті рішень лише у випадках, якщо це: необхідно для укладання або виконання договору; дозволено законодавством ЄС або держав-член, що застосовується до контролера даних; надана згода особи.

Якщо буквально тлумачити норму: «необхідно для укладання або виконання договору», то мало вірогідно, що вона саме уповноважує застосування алгоритмів для прийняття рішень. Дійсно, укладання договору страхування, кредитного договору потребує оцінки ризику, водночас складно

собі уявити, щоб ризик обов'язково оцінювався за допомогою автоматизованої системи. Тож таке положення як «необхідність» може тлумачитися як «дозвільна» вимога для укладання договору за допомогою системи алгоритмізованих рішень.

Так Федеральний закон Німеччини про захист даних, який імплементує положення Регламенту ЄС 2016/679 в національне законодавство, передбачає ст. 54, що прийняття індивідуальних рішень, заснованих виключно із використанням систем алгоритмів, які несуть юридично значущі наслідки для суб'єктів даних можна застосовувати, якщо це допускається законодавством [513]. Відповідно до ст. 42 Закону Нідерландів про захист персональних даних, передбачається дозвіл на використання системи алгоритмізованого прийняття рішень, яке базується на законі, в якому встановлюються заходи для захисту законних інтересів суб'єкта даних [862]. Згідно з п. 13 ч. 2 ст. 8 Закону України «Про захист персональних даних» передбачено право суб'єкта даних знати механізм автоматичної обробки персональних даних.

Формулювання ст. 22 Регламенту ЄС 2016/679, яка передбачає додаткові гарантії та обмеження для діяльності, що підпадає під її дію, науковці, П. Дейвіс та С. Швемер оцінюють як досить об'ємні та складні для адекватного тлумачення. Що створює перешкоди для розробників технологій [454, с. 6].

Поряд із тим, що застосування профілювання стосується захисту персональних даних, наразі Регламент ЄС 2016/679 певною мірою врегулював питання прийняття рішень із застосуванням автоматизованих систем та алгоритмів. Наразі істотною проблемою застосування алгоритмізованих рішень залишається – низький рівень обізнаності суб'єктів даних щодо збору та обробки персональних даних та способів їх використання в майбутньому, можливість застосування по відношенню до них технологій профілювання та автоматизованого прийняття рішень. Разом з цим, це є не єдиною проблемою застосування алгоритмів [216, с. 34].

Поряд із цим, слід взяти до уваги, що Регламент ЄС 2016/679 регулює застосування автоматизованих систем прийняття рішень лише в мірі, якій це

стосується обробки персональних даних. Це означає, що системи автоматизованого прийняття рішень, які не обробляють персональні дані, наприклад, використовуються для промислових завдань, обробляють анонімізовані дані, не підпадають під дію законодавства про захист персональних даних та Регламент ЄС 2016/679.

Поширення використання алгоритмів певною мірою пов’язується зі здатністю систем ШІ передбачати, оцінювати майбутні події, поведінку фізичної особи на підставі аналізу персональних даних та вчинків у мережі.

Наразі в Україні проводяться окремі кроки на шляху правового регулювання використання автоматизованих систем при прийнятті юридично значущих рішень та аналізу великих даних. У Проєкті Стратегії розвитку Верховного Суду на 2023-2027 роки в п. 13 серед іншого названо, що Верховний Суд сприяє цифровій трансформації правосуддя, будучи судом високих технологій застосовує в роботі штучний інтелект, зокрема для забезпечення єдності практики [205]. У ст. 16 Кодексу суддівської етики, затвердженого XX Рішенням з’їзду суддів України від 18.09.2024, передбачено, що використання суддею технологій штучного інтелекту є допустимим, якщо це не впливає на незалежність та неупередженість судді, не стосується оцінки доказів і процесу ухвалення рішень та не порушує вимог законодавства [76]. Вочевидь така норма носить вельми абстрактний характер, не конкретизуючи межі, стадії, на яких дозволяється використання, не називає авторизовані програми та потребує подальшого роз’яснення.

Суддя Касаційного адміністративного суду у складі Верховного Суду Я. Берназюк актуалізує питання щодо складання первинних проєктів документів із використання ШІ в роботі судді [6]. Суддя наголошує, що автоматизовані системи мають залишатись саме допоміжним інструментом, який не замінює роль судді[7].

У цьому аспекті П.А. Прохоров пропонує виділяти два типи використання ШІ при ухваленні судових рішень: допоміжний, відповідно до якого ШІ асистує судді при ухваленні судового рішення (проводить порівняльний аналіз різного

роду нормативних актів, підбирає релевантну судову практику, визначає правові позиції, від яких суд відступив тощо); ШІ як заміна судді, відповідно до якого програма самостійно на основні завданих алгоритмів приймає судове рішення[169, с. 13]. Наразі використовуються саме допоміжні алгоритмізовані системи прийняття рішень, які покликані допомогти судді під час прийняття рішень.

Слід зазначити, що система «Електронного суду», впроваджена в Україні не є штучним інтелектом, адже не використовує систему машинного навчання, як зазначає М.Р. Чалабієва [272, с. 95].

Не можна оминути Ухвалу від 08.02.2024 у справі № 925/200/22, де Верховний Суд визнав подання представником позивача заяви про роз'яснення постанови Верховного Суду від 11.12.2023 у справі, зловживанням процесуальними правами та залишив заяву без розгляду [256]. Верховний Суд зазначив, що дії заявника в сукупності, зокрема апелювання до «позиції» штучного інтелекту ChatGPT, згенерованого ним у відповідях з окремого питання, що вже розглянув суд, є виявом неповаги до суддів. Верховний Суд наголосив, що штучний інтелект може бути корисним та допоміжним інструментом у сфері правосуддя, але не може замінити роль суддів[120]. На підтримку даної позиції хочеться зазначити, що кількість невдалих випадків використання ChatGPT у практиці адвокатів та суддів, наразі, зростає. Так, юристи з США були оштрафовані за використання ChatGPT, який цитував та посилався на вигадані судові справи[839]. Аналогічна ситуація трапилася з юристами з Канади, де ChatGPT вигадав справи [365]. Про перспективи використання автоматизованих систем у судочинстві зазначається в роботах вітчизняних правників, серед яких слід назвати: О.В. Шевчука [274, с. 224], І.В. Басиста [1, с. 19], Ж.В. Удовенко [248, с. 188], Р.В. Пода [132, с. 436], І.В. Скляренко [195, с. 153], Р. Вакуліна [20, с. 88] та інших. Зрештою науковці солідаризуються та підтримують інструментальний підхід відносно застосування автоматизованих систем у судочинстві. Поряд із цим відомий український правник С.А. Чванкін виділяє дві форми участі ШІ в судочинстві.

Перша форма передбачає повну автоматизацію прийняття рішення в окремих категоріях справ, наказного провадження, де відсутній спір про право, а основна роль судді полягає в підтвердженні або запереченні вимог. Друга форма передбачає використання ШІ як помічника судді [273, с. 318].

З урахуванням зазначеного, актуалізується положення Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. Концепція передбачає винесення судових рішень у справах незначної складності (за взаємною згодою сторін), на основі результатів аналізу, здійсненого з використанням технологій штучного інтелекту, стану дотримання законодавства та судової практики [79]. Вища рада правосуддя в листі «Про погодження проєкту розпорядження Кабінету Міністрів України «Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні» із зауваженнями» від 9.02.2021 № 283/0/15-21 пропонує для реалізації заходів Концепції створення пілотного проєкту на базі суду першої інстанції в частині автоматизованого розгляду системою із застосуванням штучного інтелекту в судових справах з формальним складом. Запропоновано передати на розгляд автоматизованих систем без участі суддів, правопорушення, передбачені статтями 14-2, 122, 152-1 Кодексу України про адміністративні правопорушення [163]. Слід зазначити, що застосування автоматизованих систем у судочинстві потребує уважного дослідження та врахування наслідків і ризиків, що буде проведено далі. З урахуванням зазначеного, можна стверджувати про поступове впровадження застосування автоматизованих систем у судочинстві в Україні.

Положення *ст. 22* Регламент ЄС 2016/679 імплементовано в законодавство Франції. Відповідно до ст. 47 Закону Франції про інформатику, картотеки та свободи 1978 року, прийняття судових рішень, які передбачають оцінку поведінки фізичної особи, не можуть ґрунтуватися на автоматизованій обробці персональних даних, що має на меті оцінку окремих аспектів особи. Так, Закон Франції Про цифрову республіку застережує, що процедури примирення, посередництва, які проводяться онлайн, не можуть ґрунтуватися виключно на

алгоритмічній або автоматизованій обробці [630]. Відповідно використання алгоритму для оцінки поведінки особи в межах судового процесу не заборонено повністю, але результати аналізу алгоритму не можуть бути єдиною підставою для прийняття рішення.

Поряд із цим, законодавство Франції передбачає електронний доступ до судових рішень, що припускається, може стати базою для розвитку систем ШІ. Хоча ШІ може передбачити майбутній результат, він не здатний надати належне правове аргументування та проаналізувати складні правові ситуації, де загальне правило застосовується до конкретного випадку. Поряд із розвитком додатків для розв'язання схожих правових питань, які аналізують минулі судові рішення, що є актуальним у державах загального права, в континентальній правовій системі рішення суддів не мають силу прецеденту та судова практика залишається динамічною.

На погляд П. Дейвіса та С. Швемера, одним з аспектів ст. 22 Регламенту ЄС 2016/679 та застосування автоматизованих систем при прийнятті юридично значущих рішень є розуміння терміна «рішення». Питання полягає в тому, чи слід розглядати дії або результати таких автоматизованих операцій з обробки даних як самостійне «рішення» (в доповнення до остаточного рішення за участі людини). У разі визнання самостійності такого «рішення», на компанії, які використовують автоматизовані системи, має покладатися додаткова відповідальність [454, с. 7].

Ключовим аспектом для контролера, що автоматизує прийняття рішень, є не міра значущості людини в ухвалені рішення, а практичний ефект впливу автоматизованого рішення на суб'єкта даних.

Л.А. Байгрейв зазначає, що ухвалення рішення стосовно особи зазвичай передбачає вираження певної позиції, яка передує ухваленню самого рішення [451, с. 67].

Генеральний адвокат Суду ЄС Пікам'яе виразив позицію у справі Schufa Holding and Others про те, що вирішальним фактором є ефект, який здійснює «рішення» на суб'єкта. Компанія, що використовує систему автоматизованого

прийняття рішень, повинна оцінити можливість попередніх, повністю автоматизованих етапів, істотно вплинути на суб'єкта даних та призвести до правових наслідків. У справі Schufa Holding and Others Пікам'яе зазначає, що автоматичний розрахунок кредитного бала безпосередньо може виступати як «рішення» для цілей ст. 22(1), незважаючи на те, що остаточне рішення про видачу кредиту ухвалюються людиною. Згідно з думкою Пікам'яе, вирішальним чинником є ефект, який «рішення» здійснює на відповідну особу. Оскільки низький кредитний бал безпосередньо може мати несприятливі наслідки для особи, а саме обмежити її в здійсненні прав або, навіть, затаврувати в суспільстві, видається виправданим кваліфікувати його як «рішення» в розумінні ст. 22 (1), коли фінансова установа надає йому першочергового значення у своїй процедурі ухвалення рішень [725]. Наразі остаточне рішення у справі ще не винесено, однак, будучи потенційно знаковою, справа має внести певну правову визначеність для юридичної спільноти відносно застосування систем автоматизованого прийняття рішень, захисту даних та прав суб'єктів даних.

Законність рішень, які приймаються з використанням алгоритмів, дедалі більше стає предметом розгляду в судах США. У Х'юстоні результати таємного застосування алгоритму для оцінки ефективності роботи та впливу вчителів на учнів були використані для звільнення вчителів. Алгоритм, який використовувався, був частиною освітньої системи рейтингу вчителів, створеної технологічною компанією SAS. За твердженням суду, система не давала пояснень, яким чином вчителю підвищити рейтинг. Водночас функціонування алгоритму як програмного забезпечення, охороняється правом інтелектуальної власності та не розголошується. Суд виніс рішення про порушення прав вчителів через необґрунтованість та непрозорість рішень системи [857].

У системі кримінального судочинства США на різних етапах запроваджено понад 60 автоматизованих систем, серед яких: PSA (Public Safety Assessment) та COMPAS (Courcional Offender Management Profiling for Alternative Sanctions)[555]. Використання алгоритмів прогнозування поведінки людини піддається критиці, оскільки прогностичний результат може бути

недостовірним. Відтак саме використання суддею прогностичного алгоритму при прийнятті рішення по суті, може нівелювати здійснення права на справедливий суд, зокрема в разі буквального тлумачення рекомендації алгоритму [337, с. 60]. Приміром, в умовах перевантаженої судової системи як в Україні, перед фізичною особою постає висока спокуса використати пропозицію, згенеровану алгоритмом. Власне ідея застосування алгоритмів у судовій системі має на меті її розвантаження. Безумовно, подібні рішення впливають на здійснення прав фізичних осіб та можуть бути оскаржені. Як наприклад, справа State v. Loomis, 2017 року, де обвинувачений Е. Луміс оскаржив рішення, прийняте із використанням алгоритму. Програма аналізує окремі факти та обставини справи та дає особі оцінку, з урахуванням якої суддя може прийняти рішення. Алгоритм не дає роз'яснення та розуміння чинників, які враховувалися при оцінці поведінки особи. Технологія алгоритмізованого прийняття рішення COMPAS, яка використовується у США, належить приватній компанії, є конфіденційною. Водночас Е. Лумісу було відмовлено в роз'ясненні прийнятого рішення. Представники обвинуваченого в суді стверджували, що програма є недосконалою, приймає узагальнені висновки, дискримінаційні та не розкриває всіх критеріїв оцінки підсудного. Перед судом постало питання допустимості меж використання алгоритму для передбачення поведінки суб'єкта. Суд зазначив, що алгоритмічна оцінка може не братися до уваги та перевага віддаватися іншим доказам, водночас за будь-яких умов рішення має бути обґрунтованим та містити посилання на використанні інструменти. Суд зазначив, що права Е. Луміса дотримані, якщо прийняте судове рішення не засновано лише на оцінці, проведеній алгоритмом [417].

Слід зазначити, що основним аргументом на користь використання алгоритмів під час прийняття рішень називалось зниження упередженості та суб'єктивності властивих людині[346, с. 210]. Наразі аналіз прийняття судових рішень за допомогою алгоритмізованих систем свідчить про неупереджені та дискримінаційні рішення алгоритмів, зокрема у США. Зокрема неупередженість виявляється при використанні програми COMPAS [484]. Результати перевірки

показали, що система, яка використовувалася у штатах Арізона, Колорадо, Делавер, Кентукі, Луісіана, Оклахома, Віргінія, Вашінгтон, Вісконсін проводила дискримінаційну оцінку за ознаками раси. Разом з цим, логіка прийняття рішень програмою та прогнозування рівня ризику залишилися в таємниці [310].

Використання судами алгоритмів, критерії та логіка прийняття рішень яких залишається невідомою, ставлять ризики порушення права на здійснення правосуддя та рівність учасників процесу. Професор Каліфорнійського університету Берклі, фахівець з експертизи діпфейків Х. Фарід застерігають про негативні наслідки використання предикативної аналітики, в тому числі у кримінальному судочинстві [484; 485; 510]. Використання інструментів аналізу даних та предикативних алгоритмів як в судах, так і під час прийняття управлінських рішень має бути прозорим для суб'єктів. Непрозорість прийняття доленосних рішень алгоритмом у кримінальному провадженні ставить під сумнів дотримання прав людини.

Доки буде зберігатися проблема «чорної скриньки», яка не розкриває критерії, якими керується система, людина буде залишатися вразливою та будуть існувати ризики дискримінації [232, с. 34]. Адже лише людина ладна звернути увагу на неочевидні мотиви вчинення злочину та оцінити чинники особистого характеру, які система ШІ не здатна врахувати.

Слід зазначити про проблему упередженості алгоритмізованих систем, про які наголошує Резолюція Європарламенту про ШІ [313]. Сутність алгоритмізованої системи машинного навчання нагадує отруєне плодовите дерево, якщо відразу були здійснені неправильні кроки, то весь ланцюжок, отримані плоди та похідні результати будуть отруєні. Оскільки від того, на яких даних навчається система машинного навчання, так би мовити, що їй «згодовують», напряму залежить отримуваний результат. Особливо це стосується випадків, коли не відома логіка роботи системи та не відомі, які дані обробляє система.

Крім того, набір цінностей, які відтворює алгоритмізована система, відображає цінності та точки зору, які існують в суспільстві. Зрештою, така точка зору набуває еталонного значення.

Як зазначила у своїй промові у 2021 році керівник Інформаційного комісара Великобританії Є. Данем, інформаційні технології, що розвиваються, перетворили дані на ключовий актив, що вимагає інвестицій, захисту та поваги, щоб розкрити їх впливову цінність. Належний захист даних гарантує, що успішність впровадження інновацій, де суб'єкти можуть довіряти компаніям та державним органам в тому, що використання даних відповідає закону. За своєю суттю захист даних заснований на довірі. Правове регулювання захисту даних стали запроваджувати у 1970-х роках саме через побоювання втручання технологій у приватне життя. Заплановані інновації, засновані на даних, будуть успішно функціонувати лише у випадку, якщо люди будуть готові поділитися своїми даними, будучи впевненими, що їх буде використано справедливо [568]. Наразі ключовим чинником розвитку технологій стає прозорість та довіра технологіям. Але слід зазначити, що поряд із реальними ризиками застосування технологій, набувають істотного значення й гіпотетичні ризики, про які люди думають, що вони існують, адже в результаті вони також впливають на зниження рівня довіри користувачів.

Аналогічно зазначається у Рекомендаціях ЮНЕСКО про етичні аспекти ШІ, що: розвиток систем на основі ШІ порушує етичні питання, зокрема щодо їх впливу на процеси ухвалення рішень у різних сферах суспільства та дотримання прав людини та основоположних свобод, включно зі свободою вираження поглядів, недоторканністю приватного життя та відсутністю дискримінації [712].

Стандарти, шаблони існують у будь-якому суспільстві, водночас саме в алгоритмізованих системах як і в будь-яких алгоритмах, упередження зводяться у високий ступінь, еталон та здатні призводити до негативних наслідків.

Можна навести приклад чатбота Тея, розробленого Майкрософт, що навчився на реальних даних у Твіттері, аналізуючи та беручи участь у спілкуванні із користувачами. Врешті Тей став виражати розгнівану, расистську

поведінку, нетерпимість та ворожнечу. У певному сенсі Тей є невдалим проєктом, який відобразив всі негативні властивості користувачів під час спілкування в мережі. Адже алгоритми вивчають структурні упередження, нерівність у суспільстві та відображають цю дискримінацію [314].

Тож означену модель поведінки алгоритм сприйняв як домінуючу, та відтворив як взірцеву. Врешті розробники Microsoft видалили чатбот та вибачилися. Означене ілюструє, що фахівці мають враховувати при розробці систем побічний ефект великих чисел.

У цьому сенсі, інтерес привертає дослідження Д. Чена, який аналізує можливості та шляхи використання систем машинного навчання для виявлення та попередження упереджень у судовій системі. Науковець провів аналіз рішень декількох суддів США. За твердженням науковця за допомогою алгоритмів можна виявляти негативні явища двох видів: коли судді не беруть до уваги юридично значущі обставини справи та коли судді беруть до уваги обставини, які не мають юридичної значущості або коли такі обставини на мають вплив. Науковець зазначає, що на прийняття рішення можуть впливати обставини, які не стосуються справи (погода, результати футбольних матчів, свята, день народження родичів). За допомогою використання алгоритмів, науковець розмежував суддів залежно від рівня вірогідності передбачити остаточне рішення, які вони приймуть: із високим рівнем передбачуваності, коли від початку можна передбачити остаточне рішення та вплив зовнішніх чинників, не поглиблюючись у суть справи; з низьким рівнем передбачуваності [427, с. 6]. Даний приклад алгоритмічного аналізу може бути використаний для попередження про можливість винесення упередженого рішення та підсвічувати, навчати, нагадуючи про існуючі, вірогідні упередження. Можна зробити висновок, що алгоритмічний аналіз та система машинного навчання можуть допомогти виявити упередження.

Особливістю алгоритмічних структурних упереджень є те, що вони відображають упередження, які існують у реальному житті, можуть бути виявлені та відтворені автоматизованою системою.

Поряд із структурними упередженнями алгоритмів, упередження автоматизації не лише відтворюють упередження фізичного світу, а й фактично впливають на образ мислення суб'єкта та прийняття рішень, навіть у тих випадках, коли він усвідомлює, що стикається із упередженням. Упередженість автоматизації є тенденцією надмірно покладатися на рішення, прийняті алгоритмом [539, с. 123]. Відомі випадки, коли в період поширення Covid-19 система розпізнавання обличчя, встановлена на об'єктах транспортної структури в одному із мегаполісів світу, розпізнала людину як таку, що перебуває в розшуку, при цьому співробітниками поліції, які знаходилися на місці, було очевидно, що людина, яку вони затримали, не схожа на особу, яка перебуває в розшуку. Упередження автоматизації виявилося в тому, що співробітники поліції, навіть розуміючи абсурдність затримання, віддали перевагу довіряти рішенню алгоритму, аніж власним очам, уявленням про справедливість та законність.

Наслідком упереджень, нерозуміння функціонування системи «чорної скриньки», коли особі невідомо, на яких підставах алгоритм прийшов до певного рішення, коли особа намагається підвести будь-яку логіку під прийняте рішення алгоритмом, намагається підігнати правдоподібне логічне пояснення під рішення алгоритму, яке не має розумних підстав обґрунтування, – є алгоритмічне або математичне відмивання («mathwashing» або «farewashing) [357]. Термін, запропонований американськими фахівцями, передбачає ситуацію, коли людина перестає довіряти собі, а автоматично обирає довіряти програмі, нехтуючи критичним мисленням. Математичне відмивання виникає внаслідок надмірної ідеалізації діяльності алгоритмів. Т. Шеп відрізняє математичне відмивання: яке відбувається випадково (людина не розуміє вразливість рішення алгоритмічної системи) або проводиться цілеспрямовано (коли особа дотримується вочевидь упередженого рішення, прийнятого системою). Цілеспрямоване слідування упередженому рішенню може бути обумовлено тим, що особа побоюється публічного осуду, бажає зберегти репутацію, хоча для суспільства є очевидним упередженість алгоритму [864]. Цілком слушним є застосування терміна

«алгоритмічне або математичне відмивання» в українській правовій доктрині та практиці.

Проблема постає і з розумінням упередженості як такої, оскільки стандарту упередженості не існує, і також варіюється залежно від історичних, територіальних чинників, соціальних груп, релігійної приналежності, статі тощо. Так, наприклад, 100 років тому не визнавалося упередженістю недопущення жінок до певних професій, посад, або позбавлення права голосу, оскільки це було звичайною ситуаціє для того часу. Водночас сьогодні встановлення будь-яких обмежень щодо обіймання жінками певних посад або зайняття певною діяльністю, буде визнано упередженістю. Прикладом упередженості для більшості цивілізованих держав світу також є різний обсяг прав осіб, в залежності від релігії. Провідною умовою, що під час розробки та роботи алгоритма є недопущення різного ставлення та надання різного обсягу прав по відношенню до людини, соціальної групи, якій вона належить.

Відтак на функціональність алгоритму впливають цінності та культура, до якої належать його розробники. За визначенням Н. Бострома, Е. Юдковського, якщо б у розробці алгоритму брав участь Архімед, то на нього впливали б давньогрецькі цінності, устрій та етичні норми, зокрема прийняття рабства [345, с. 60]. Тож під час проєктування, розробки, тестування автоматизованої системи (продукту) розробники, інженери можуть впливати, вносити уточнення (свої упередження) у функціонування системи під час всього циклу розробки.

Як зазначає О.Е. Радутний, дослідник застосування великих даних у кримінальному праві, кореляцій на підставі обробки великих даних можуть: впливати на рішення, які приймаються людиною; доповнювати аргументацію для обґрунтування рішень; суперечити рішенням, які приймаються людиною, з огляду на знання та отриманий досвід [173, с. 96]. Тож під час прийняття юридично значущих рішень має братися до уваги, що остаточне рішення має приймати саме людина, адже система може прийти до упереджених результатів.

Підсумовуючи викладене, ми пропонуємо розрізняти: упередження в структурі або архітектурі системи, які є наслідком функціонування алгоритму,

можуть бути випадковими, несвідомо привнесені розробниками внаслідок не взяття до уваги особливостей функціонування алгоритму; упередження в даних відбуваються внаслідок функціонування системи, яка виводить певне значення на рівень еталону (внаслідок низького рівня якості даних, не взяття до уваги належної репрезентативності); упередження, обумовлені використанням системи, що особа надмірно покладається на рішення, прийнятті алгоритмом, нехтуючи власним досвідом та критичним мисленням.

Неможливість встановити підстави прийняття рішень алгоритмічними системами, впровадження використання автоматизованих систем, упереджень актуалізує виклики для справлення та забезпечення верховенства права. Приклади із практики США свідчать про безуспішність створення алгоритму, який би ефективно подолав упередження. Оскільки система від початку навчається на некісних даних, які містять упередження, існуючі у реальному світі.

Слід підсумувати, що незважаючи на те, що остаточне рішення в таких сферах як фінанси, працевлаштування, судочинство, наразі ухвалюються за участю людини, ефект, який попереднє рішення автоматизованої системи здійснює на відповідного суб'єкта даних, сам по собі може мати несприятливі наслідки для особи суттєво обмежувати здійснення прав або навіть затаврувати, оскільки суб'єкт прийняття юридично значущого рішення надає рішенню автоматизованої системи першочергового значення у своїй процедурі ухвалення рішень.

Європейська спільнота традиційно вимогливо ставиться до питань дотримання прав людини та послідовно впроваджує засади суворої регламентації застування алгоритмізованих систем та штучного інтелекту. Біла книга із штучного інтелекту ЄС від 19.02.2020 дотримується людиноцентричного підходу, ризик орієнтованого підходу до використання новітніх технологій та приділяє увагу етиці застування ШІ [866]. Міністерством цифрової трансформації України була розроблена Біла книга з регулювання ШІ в Україні (версія для консультації) у 2024 році, яка передбачає такі заходи для

подолання ризиків: добровільне маркування систем ШІ для побудови довіри, демонстрації підзвітності та відповідальності розробників; розробка та добровільне дотримання кодексів поведінки компаніями, які розробляють та використовують ШІ; прийняття заходів для уникнення упереджень та дискримінації тощо [9].

Біла книга із Штучного інтелекту Європейської Комісії називає такі ключові групи ризиків від використання алгоритмів: ризики для основних прав, включаючи захист персональних даних та приватне життя; дискримінацію та ризики для безпеки та ефективного покладання відповідальності [866].

У документі Дослідницької служби Європейського парламенту «Штучний інтелект»: Як він працює, чому це важливо і що ми можемо з цим зробити?» пропонується виділяти: існуючі виклики використання ШІ для прав людини та гіпотетичні виклики. Серед існуючих викликів використання ШІ називається: 1) непотрібне недовикористання; 2) проблема прозорості: (недостатня пояснюваність функціонування алгоритмів; незбалансований доступ до інформації; необізнаність людей про взаємодіють із ШІ; 3) непрозорість інформації про потенційні наслідки та відсутність довіри та опір суспільства, відсутність розуміння як функціонує алгоритм; 4) проблема виявлення достовірних фактів та фейків; 5) упередженності; 6) узгодження цінностей; 7) конкуренція; 8) розподіл доходів та витрат від використання систем; 8) ризики для безпеки під час ведення воєнних дій та вторинного використання; 9) небезпечне надмірне використання (застосування ШІ для вирішення завдань, для яких він не застосовуваний, а саме: встановлення причинно-наслідкових зв’язків, прогнозування індивідуальних результатів у складних соціальних системах); 10) застосування ШІ для розв’язання завдань, для яких він добре підходить, але призводить до виникнення вразливостей суб’єктів даних [314]. Серед гіпотетичних викликів ШІ називаються: утопічні та антиутопічні сценарії; зима ШІ; набуття системою здатності контролювати власний розвиток та втрата людиною контролю над системою; втрата робочих місць; втрата людиною власної автономії; набуття свідомості та автономії системами.

З урахуванням вищевикладеного, можна назвати такі виклики, які безпосередньо стосуються недоторканності приватного життя: технології та системи ШІ наслідують упередженості своїх розробників; моделі можуть бути несправедливими та дискримінаційними, тому що навчальні дані містили упереджені переконання; дискримінація може бути результатом закономірностей, які виявляє система ШІ; непрозорість «чорної скриньки», яка ускладнює розуміння того, як виявляються закономірності та кореляції в певному процесі; розкриття повної логіки про функціонування програми, автоматизованої системи ШІ може призвести до розкриття комерційної таємниці розробників, яка є об'єктом інтелектуальної власності та відповідно захищається; мета збору та обробки великих обсягів персональних даних, яка може змінюватися; неможливість передбачити результат навчання системи.

Слід взяти до уваги, що чим більш розвинута правова система, юрисдикція, тим більш значущу роль відіграють загальні принципи права, а з тим, більше вона є продуктом права, а не букви, тим більш значущу роль буде відігравати дух права, цілі правового регулювання, над конкретним нормативним формулюванням, нормою права, яку може сприймати та адекватно тлумачити лише людина, а не алгоритм. Крім того, судами в розвинених юрисдикціях беруться до уваги під час прийняття рішення такі, не суто юридичні чинники як: економічний благоустрій суспільства, морально-етичні чинники, підтримання стабільності правової системи тощо. У цьому сенсі доречно навести висловлення британського правника лорда Т. Бінгема, що суть принципу верховенства права полягає в тому, що всі суб'єкти та органи влади мають бути пов'язані та уповноважені законами, публічно й завчасно оприлюдненими та публічно застосовуваними в судах [11; 129, с. 134]. Т. Бінгем вивів принципи верховенства права: 1) право має бути доступним, зрозумілим, ясним і передбачуваним; 2) питання права та відповідальності зазвичай мають вирішуватись шляхом застосування закону, а не на розсуд; 3) право має застосовуватися однаково до всіх, за винятком випадків, коли об'єктивні відмінності виправдовують диференціацію; 4) закон повинен забезпечувати адекватний захист основних

прав людини; 5) закон має давати сторонам можливість розв'язувати правові спори, які вони не здатні вирішити самостійно, без непомірних витрат або надмірних затримок; 6) державні службовці всіх рівнів повинні здійснювати надані їм повноваження розумно, сумлінно, з метою, для якої ці повноваження було надано, і не виходячи за межі цих повноважень; 7) судові процедури, які надаються державою, повинні бути справедливими; 8) держава повинна дотримуватись своїх зобов’язань за міжнародними нормами і стандартами, які вона взяла [332].

Можна зазначити, що дані принципи відображають далекоглядну логіку європейського правника, яку можна простежити під час розробки нормативно-правових актів, щоб упередити хаотичні зміни до них, забезпечити стабільність для розвитку відносин та бізнесу.

Т. Огнев’юк зазначає, що попри те, що зупинити розвиток систем ШІ як елемента технологічного прогресу неможливо, потребує розробки законодавчого врегулювання його застосування для недопущення порушення основних прав і свобод, та гарантування верховенства права [119, с. 66].

Серед конкретних способів подолання викликів ШІ документ Дослідницької служби Європейського парламенту «Штучний інтелект» пропонує: запровадити механізми, які забезпечать можливість перегляду людиною рішень, ухвалених алгоритмами; фізичним особам надати право знати, якою мірою продукти, послуги, які вони споживають, виробляються та надаються ШІ, що включає повідомлення про те, що суб’єкт піддається автоматизованій обробці під час прийняття рішення та повідомлення про взаємодію із ШІ.

У 2021 року Комісією ЄС була внесена пропозиція до Європейського Парламенту та Ради прийняти Гармонізовані правила щодо штучного інтелекту та внести зміни до деяких законодавчих актів Союзу [752], в якій приділено увагу ефективному застосуванню законодавства та дотриманню прав людини в умовах розвитку ШІ. Ризик застосування розробок нових та потужних технології не за призначенням, з метою маніпулювання, експлуатації та соціального контролю

викликає занепокоєність та з огляду на невідповідність подібної практики загальноєвропейським цінностям прав людини її пропонується заборонити.

Акт ЄС Про ШІ передбачає правила розмежування систем штучного інтелекту залежно від ступеня ризику. До категорії систем штучного інтелекту із високим ступенем ризику віднесено: скорінг під час працевлаштування, дистанційна біометрична ідентифікації в режимі реального часу, предикативні системи судочинства. Відповідно до ст. 113 Акту ЄС про ШІ, забороненими визнані такі види діяльності з ШІ: маркетинг, введення в експлуатацію або застосування систем штучного інтелекту, які використовують сублімінальні методи впливу на підсвідомість, що можуть завдати фізичну або психологічну шкоду людині; маркетинг, введення в експлуатацію або застосування систем штучного інтелекту, які використовують буд-які вразливі риси, пов'язані з віком, фізичні або розумові недоліки осіб (групи осіб) для впливу на їх поведінку, що може завдати фізичну або психологічну шкоду людині; маркетинг, замовлення або використання державними органами або від їх імені систем штучного інтелекту призначених для оцінки або ранжування надійності осіб протягом певного періоду часу на підставі аналізу їх соціальної поведінки, або прогнозованих здібностей (соціальна оцінка може призводити до упередженого ставлення до осіб в аспекті, не пов'язаному з отриманими даними); використання систем дистанційної біометричної ідентифікації в режимі реального часу в публічних місцях з метою правоохоронної діяльності; використання автоматизованих систем, які створюють або розширюють бази даних біометричної ідентифікації шляхом нецільового збору даних з відкритих джерел в інтернеті, або записів з камер відеоспостереження; використання систем ШІ для впливу на емоційний стан фізичної особи на робочому місці та в навчальних закладах; використання систем біометричної ідентифікації для ранжування градації та визначення або припущення щодо раси, політичних поглядів, членства у профспілкових організаціях, релігійних чи філософських переконань, приватного життя.

Як зазначають Дж. Гакутан, Н. Сельвадурай, непрозорість прийняття рішень, втаємничення логіки їх прийняття системою та відсутність можливості отримати пояснення зацікавленими особами, ставлять потребу запровадження в законодавстві права на тлумачення алгоритмізованих рішень та їх оскарження у випадку, якщо вони порушують право на недоторканність приватного життя та право на гідність. Відтак відсутність прозорості, оцінка та прийняття рішень без розкриття обґрунтування таких рішень ставить під загрозу право на недоторканність приватного життя та гідність особи [528, с. 195]. Для забезпечення прозорості рішень та ефективного контролю за системами автоматизованого ухвалення рішень суб'єкта даних має бути надано право на роз'яснення рішень відносно нього, зокрема тих, які стосуються долі суб'єкта.

На погляд Б. Гудмана, С. Флаксмана, здійснення «права на роз'яснення» суб'єктам даних може стати тягарем для компанії, які використовують системи обробки великих для прийняття юридично значущих рішень та предикативну аналітику, водночас пред'являє вимогу вжити заходи для прозорості системи та недопущення дискримінації [541].

З урахуванням викладеного, слід констатувати існування різних підходів здійснення права на роз'яснення рішення, прийнятого за допомогою штучного інтелекту у США та ЄС. Традиційно держави ЄС приділяють значну увагу дотриманню прав та свобод людини, а вимоги забезпечення прозорості діяльності органів державної влади та виконання обов'язків контролерами із розкриття певних даних, передбачених у положеннях держав членів. Тож для надання громадянам певного захисту від алгоритмізованих систем, забезпечення прозорості та певного контролю за алгоритмами, французьке законодавство передбачає, що правила, які визначають засади алгоритмізованої обробки, мають бути оприлюднені на державному сайті (Закон Про цифрову республіку від 7 жовтня 2016 року) [630]. Принципи, прозорість функціонування систем автоматизованого прийняття рішень наділяють суб'єктів даних правом оскаржувати несправедливі рішення або ті, які є дискримінаційними.

Науковцями висуваються різні позиції щодо тлумачення норми ст. 22 Регламенту ЄС 2016/679. Одні науковці Г. Малгєрі, Дж. Команде, А. Селбста дотримуються широкого тлумачення норми ст. 22 та покладають на контролерів обов'язок, у разі використання алгоритмів при прийнятті юридично значущих рішень, розкривати суб'єкту даних повну інформацію про логіку, алгоритм прийняття рішення, навіть технічну складову [646, с. 243].

Прибічники протилежної позиції С. Вахтер, Б. Міттельштадт, Л. Флоріді, Т. Кім, Б. Рутледж стверджують, що відповідно до змісту ст. 22 Регламенту ЄС 2016/679 контролери не зобов'язані надавати детальну інформацію про алгоритм прийняття рішення, а обмежені повідомленням загальної інформації, без обов'язку розкриття деталей функціонування алгоритму. Дана позиція ґрунтується на відсутності конкретизованої інформації, яку має розкрити контролер фізичній особі за Регламентом ЄС 2016/679 [850, с. 80]. Крім того, ст. 22 містить застереження, що вона застосовується в разі, коли система приймає рішення самостійно, без будь-якого втручання людини.

До того ж практика імплементації Регламенту ЄС 2016/679 в національне законодавство членами ЄС свідчить, що переважна кількість держав уникають застосування розширювального підходу, який зобов'язує контролерів надавати суб'єктам даних докладну інформацію про функціонування алгоритмів [646, с. 245; 647, с. 2; 648, с. 125]. Серед держав, які передбачили обов'язок розкриття логіки прийняття рішення, слід навести Нідерланди, де п. 4 ст. 42 Закону про захист персональних даних передбачає, що контролер у разі прийняття рішення із застосуванням алгоритму інформує суб'єкта даних про логіку, що лежить в основі автоматизованої обробки даних щодо нього [862]. Аналіз позиції Робочої групи із захисту прав людини у сфері обробки персональних даних, викладеній у Керівництві з автоматизованого прийняття індивідуальних рішень та профайлінгу для цілей Регламенту формулювання, «рішення, засновані виключно на автоматизованій обробці» не свідчить, що у випадку формальної участі людини, контролер звільняється від обов'язку надати відповідну інформацію суб'єктам персональних даних, у разі запиту [703].

Слід також зазначити, що відповідно до п. f ч. 2 ст. 13, п. g ч. 2. ст. 14, п. h, ч. 1 ст. 15 Регламенту ЄС 2016/679 передбачено, що контролер повинен надати суб'єкту даних інформацію лише про наявність процесу автоматизованого прийняття рішення, профілювання та достовірну інформацію про відповідну логіку та наслідки рішення.

Тож буквальне тлумачення норм Регламенту ЄС 2016/679 не свідчить про обов'язок контролера розкривати докладну інформацію та логіку прийняття рішення алгоритмом. Таким чином, це питання залишається дискусійним та потребує розв'язання у правозастосовчій практиці.

За твердженням французького науковця Дж. Дюкле, в рішенні про використання алгоритму мають бути відображені способи функціонування алгоритму[487, с. 230]. Водночас М. Хільдебрандт зазначає, що в разі законодавчого закріплення вимоги прозорості функціонування систем автоматизованого прийняття рішень постає питання способу такого забезпечення, адже система або код має вигляд математичної формули, яка не є читабельною та зрозумілою для звичайного користувача. До того ж, у разі розкриття логіки функціонування системи, виникає вірогідність підлаштовування даних для отримання певного вигідного результату. Також постає питання особи, яка має бути відповідальною за помилки вчинені автоматизованою системою та досягнення незапрограмованих результатів [557, с. 180]. До того ж, з огляду на те, що по мірі самонавчання та розвитку системи зростає рівень її непередбачуваності, постає ризик, що система може змінювати налаштування по мірі зростання її винахідливості, а з тим, виникає потреба забезпечення можливості втручання в її функціонування людиною.

Згідно із дослідженням, проведеним Відділом наукового прогнозування Європейської парламентської дослідницької служби [856], що розкриття всього алгоритму вимагає значних ресурсів та не забезпечує бажаного пояснення логіки прийнятого рішень, дослідники пропонують встановлення заходів, направлених на розкриття даних про логіку прийняття індивідуальних рішень, аналізу вхідних

даних, статистичного пояснення, перевірки коду (конструкції) та статистичного аналізу, визначення чутливості окремих даних (які саме зумовили результат).

У цьому сенсі цікавим є твердження С. Вахтер, Б. Міттельштадт та Л. Флоріді, які під роз'ясненням автоматизованого прийняття рішення розрізняють: роз'яснення функціональності системи, тобто логіку, значення, передбачувані наслідки та загальну функціональність автоматизованої системи ухвалення рішень, наприклад, специфікацію вимог системи, структуру рішення, зумовлені моделі, критерії та класифікаційні структури; роз'яснення конкретних рішень, тобто обґрунтування, причини та індивідуальні обставини ухвалення конкретного автоматизованого рішення, наприклад, коефіцієнти характеристик, правила ухвалення рішень, що визначаються системою для кожного конкретного випадку [850, с. 79]. Науковці пропонують розрізняти роз'яснення рішення залежно від того, коли воно надається по відношення до прийняття рішення: 1) роз'яснення відбувається до того, як проводиться автоматизоване прийняття рішення. Таке роз'яснення логічно може стосуватися лише функціональності системи, оскільки обґрунтування конкретного рішення не може бути відоме до його прийняття; 2) роз'яснення відбувається після ухвалення автоматизованого рішення, може стосуватися як функціональності системи, так і обґрунтування прийняття конкретного рішення.

Прикладом може бути автоматизована система кредитного рейтингу. До ухвалення рішення постачальник системи може поінформувати суб'єкта даних про функціональність системи та загальну логіку роботи системи (наприклад, типи даних і характеристики, що аналізуються), мету або значення (присвоєний кредитного бала) та передбачувані наслідки (наприклад, кредитний бал можуть використовувати кредитори для оцінювання кредитоспроможності, визначення умови кредитування та розміру відсоткової ставку). Вже після прийняття рішення суб'єкту даних може бути надано роз'яснення прийнятого конкретного рішення стосовно нього [850, с. 82].

Здається, що Регламент ЄС 2016/679 забезпечує надійний захист від автоматизованого прийняття рішень, але в нинішньому вигляді цей захист може

виявитися неефективним, з огляду на поширення застосування систем автоматизованого прийняття рішень та автоматизованої обробки даних для підтримки прийняття рішень людиною, що є прогалиною в реалізації засад прозорості та підзвітності. Можна підсумувати, що право на роз'яснення конкретних рішень юридично не передбачено гарантіями, що містяться у статті 22(3) або ст. 13, 14 Регламенту ЄС 2016/679. У нинішньому вигляді повноцінне право на роз'яснення обґрунтування та обставин прийняття конкретних автоматизованих рішень не передбачається, також не міститься конкретизація та не покладаються юридичні обов'язки на контролерів даних надавати технічну інформацію (фактично відкривати «чорну скриньку») про те, як працює алгоритм обробки персональних даних. Таким чином підходи в доктрині ЄС не передбачають розкриття повної логіки прийняття рішення.

Стосовно США, то на відміну від ЄС, де діє Регламент ЄС 2016/679, який торкається питань обробки персональних даних, прозорості алгоритмів, поширюється та вимагає дотримання всіма державами членами ЄС, в США відсутнє єдине законодавство на федеральному рівні, яке б регламентувало питання збору та обробки персональних даних, забезпечення прозорості та підзвітності алгоритмів. Якщо в ЄС у цій сфері застосовується правило: «все, що прямо не дозволено, те заборонено», тоді в США керуються принципом «все, що прямо не заборонено, дозволено».

Норми, які регулюють збір та обробку персональних даних у США, передбачені в різних нормативно-правових актах, які подекуди не пов'язані між собою на рівні федерації та штатів. Так, низка норм та підходів передбачена для недопущення дискримінації при прийнятті рішень людиною, не передбачають вичерпного переліку засобів захисту від дискримінації в разі застосування систем автоматизованого прийняття рішень [535, с. 463; 536]. Наприклад, федеральний Закон про справедливе житло 1968 року, який забороняє дискримінацію державними органами, банками, страховиками та іншими кредитними установами, забудовниками за ознаками раси, релігійних переконань, статі, національної приналежності, сімейного становища,

передбачає повідомлення кредитором заявника про обставини, які призвели до відмови у видачі кредиту [509]. Параграф 1691b Закону про рівні можливості отримання кредиту 1974 року передбачає обов'язок кредитора надати письмове пояснення причин відмови у видачі кредиту[502].

Згідно із аналогічними нормативно-правовими актами, не допускається брати до уваги під час прийняття рішень характеристики, обробку даних яких заборонена, як-то стать, расова приналежність тощо. Можна підсумувати, що правове регулювання означених питань у США практично відбувається з урахуванням специфіки кожної ситуації з дотриманням окремих норм антидискримінаційного законодавства, яке забороняє або обмежує обробку чутливих персональних даних.

Наразі вчиняються спроби забезпечення прозорості та підзвітності алгоритмізованих систем прийняття рішень у США. У 2019 році в Конгрес США представив Законопроєкт Про алгоритмічну підзвітність [298], який покладає обов'язок на осіб, які використовують автоматизовані системи прийняття рішень під час розробки, використання, проєктування та навчання цих систем проводити оцінку їх впливу на здатність дотримання таких засад як: точність, справедливість, неупередженість, недискримінаційність, конфіденційність та безпека. До наглядового органу має бути надано детальний опис, призначення, конструкцію, здатність до навчання системи автоматизованого прийняття рішень. Наразі даний Законопроєкт з доповненнями в редакції від 3.02.2022 року, знаходиться на розгляді. Аналогічний законопроєкт запропоновано у Штаті Каліфорнія. Законопроєкт містить визначення систем автоматизованого прийняття рішень як обчислювального процесу, заснованого на машинному навчанні, статистиці або інших методах обробки даних, застосуванні систем, здатних приймати рішення або полегшувати прийняття рішення людиною. Поряд зі цим, передбачається запровадження категорії «оцінки впливу автоматизованих систем прийняття рішень», що позначає оцінку впливу систем на точність, справедливість, упередженість, дискримінаційність, конфіденційність та безпеку. Також окремі штати як Нью-Йорк[816] та

Вашингтон [854] розробляють законодавство в галузі правового регулювання застосування систем автоматизованого прийняття рішень державними органами.

У Канаді приймаються нормативно-правові акти, які спрямовані на розкриття питань використання автоматизованих систем під час прийняття рішень у Монреальській декларації про відповідальний розвиток штучного інтелекту [817]. Прийнято стандарти розробки та використання систем автоматичного прийняття рішень із урахуванням етичних аспектів [506]. Використання систем автоматизованого прийняття рішень у сфері державного управління в Канаді регулює Директива з автоматизованого прийняття рішень, яка спрямована на зниження впливу негативних наслідків при прийнятті рішень на громадян Канади в разі використання ШІ та забезпечення дотримання принципів ефективності, точності, прозорості тлумачення рішень [702].

Стосовно вітчизняної практики, то Закон України «Про захист персональних даних», який передбачає право знати механізм автоматичної обробки персональних даних та право особи на захист від автоматизованого рішення, яке має для нього правові наслідки в п. 13, ч. 2 ст. 8. Тобто нині чинний Закон можна охарактеризувати як спрямований на розкриття інформації відносно функціонування алгоритму, щоб суб’єкт даних міг отримати дані про прийняте рішення, водночас не передбачає належного порядку здійснення права на роз’яснення конкретно прийнятого рішення за допомогою системи автоматизованої обробки та механізми захисту від автоматизованого прийняття рішення свідчить практика з урахуванням розвитку інформаційно-комунікаційних технологій.

Відповідно до ст. 25 Проєкту Закону «Про захист персональних даних» від 25.10.2022 № 8153, передбачається право на захист від автоматизованого прийняття рішення, яке змістом відтворює ст. Регламенту ЄС 2016/679 [140].

З урахуванням викладеного та відсутності конкретизованої інформації, яку має розкрити контролер фізичній особі за Регламентом ЄС 2016/679, вважаємо, що для належного здійснення прав суб’єктів даних, необхідно передбачити в законодавстві право суб’єктів даних на роз’яснення конкретного рішення,

прийнятого за допомогою системи автоматизованої обробки персональних даних та обов'язок контролера в разі прийняття рішення із застосуванням алгоритму, надати інформацію суб'єкту даних про логіку рішення, що лежить в основі автоматизованої обробки рішення, прийнятого щодо нього, без розкриття програмного коду.

Тому вважаємо доцільним доповнити Проєкт Закону України «Про захист персональних даних» від 25.10.2022 № 8153, який прийнятий за основу, статтею 25-1 «Право на роз'яснення та оскарження індивідуальних рішень, прийнятих за участі автоматизованих систем» таким змістом:

«1. У разі використання автоматизованої системи при прийнятті рішення, яке має юридично значущі для суб'єкта персональних даних або іншим чином здійснює істотний вплив на нього, суб'єкт персональних даних має право звернутися до контролера для отримання роз'яснення та обґрунтування обставин прийняття індивідуального рішення, прийнятого за участі автоматизованої системи.

2. Суб'єкт персональних даних має право звернутися до контролера для оскарження індивідуального рішення, яке має юридично значущі наслідки або іншим чином суттєво впливає на нього до суду, в разі його прийняття автоматизованою системою або за участі автоматизованої системи при прийнятті рішення».

Можна підсумувати, що з технічної точки зору відмінності між системами автоматизованого прийняття рішень, заснованому на машинному навчанні та сучасними нейронними мережами є досить істотними, водночас виклики та юридичні питання, які виникають у результаті використання, залишаються впродовж років незмінними [221, с. 40; 243, с. 56].

Ще одним правом, передбаченим п. 10 ст. 8 Закону України «Про захист персональних даних» та ст. 18 Регламенту ЄС 2016/679 є право на обмеження обробки персональних даних, яке можна розглядати як обов'язок контролера зберігати персональні дані, які не можна ні обробляти, ні змінювати якимось чином. Дане право застосовується у випадках, коли немає точної вказівки на те,

чи будуть видалені персональні дані на законних підставах та коли. Якщо право на видалення за ст. 17 не може бути застосовано щодо організації, яка має юридичний обов'язок зберігати дані, особа має право обмежити обробку персональних даних у таких випадках: якщо точність відповідних даних оспорюється; якщо обробка даних була незаконною, але особа виступає проти їх видалення; якщо дані необхідні для здійснення та оспорювання правових вимог; якщо особа скористалася своїм правом на оскарження відповідно до ст. 21, але контролер вимагає «переконливих законних» підстав для обробки.

Згідно з п. 2 ст. 18 Регламенту ЄС 2016/679 передбачені наслідки здійснення права особи на обмеження обробки. За виключенням зберігання, персональні дані не можуть оброблятися контролером, інакше як: за згодою зацікавленої особи; для судочинства та подання позову; для захисту прав інших осіб (преамбула 73); здійснення важливих публічних інтересів (преамбула 73).

Регламент ЄС 2016/679 не містить, яким саме чином може бути обмежена обробка персональних даних на вимогу суб'єкта даних, водночас у п. 67 Преамбули міститься вичерпний перелік методів досягнення означеної мети: персональні дані можуть бути тимчасово переміщені в іншу систему обробки, щоб зробити їх недоступними для користувачів; дані можуть бути тимчасово видалені зі сторінки. У випадку використання систем автоматизованого обмеження обробки, технічні заходи мають гарантувати, щоб персональні дані не піддавалися подальшій обробці та зміні. Обмеження обробки персональних даних має чітко відображатися в мережі. Тривалість обмеження на обробку з Регламентом ЄС 2016/679 не встановлено, водночас це має залежати від конкретних фактів та ситуації. Вочевидь суб'єкт має бути повідомлений про зняття обмежень про обробку персональних даних.

З огляду на те, що в сучасних реаліях часовий аспект має враховуватися з урахуванням швидкості змін інтересів та вподобань користувачів, а з тим і застарівання персональних даних, Б. Кастерс висуває пропозицію запровадження права на сплив строку чинності персональних даних та потребу закріпити строки для зберігання даних в інформаційно-комунікаційних

системах. Для спрощення встановлення спливу строку чинності та зберігання персональних даних, науковець пропонує встановлення трьох або п’ятирічного періоду, упродовж якого персональні данні вважаються чинними. Науковець пропонує запитувати в суб’єктів підтвердження наданої згоди на обробку, зберігання зі спливом строку чинності даних. Наразі після проходження реєстрації та отримання згоди на обробку лише подекуди платформи запитують підтвердження або оновлення персональних даних. Слід зазначити, що згідно з п. а ч 2 ст. 13 Регламенту, на контролера покладається обов’язок надати суб’єкту даних інформацію, необхідну для забезпечення неупередженої та прозорої обробки щодо строків зберігання персональних даних або критерії визначення строків зберігання даних за можливості. Крім того, відповідно до п 7.4.7 ISO/IEC 27701, прийнятого у 2019 році, контролер повинен зберігати, обробляти персональні дані не довше, ніж це необхідно для цілей, для яких вони були зібрані, розробляти та дотримуватися графіків їх зберігання, беручи до уваги вимогу зберігання не довше, ніж це необхідно за законодавством. У разі виникнення суперечностей між різними нормами законодавства щодо строків зберігання, контролер має прийняти рішення (на підставі оцінки ризиків) та оформити відповідний графік зберігання [573].

Щодо пропозиції Б. Кастерса про закріплення втрати актуальності даних хочеться зазначити, що покладання на компанії додаткового обов’язку дотримання строків чинності персональних даних, які обмежуються короткими проміжками часу як три, п’ять років, поряд із дотриманням вимог законодавства щодо обробки даних в умовах розвитку штучного ШІ є не раціональним та обтяжливим для компаній. Зрештою таке право не надає додаткових засобів захисту права суб’єктів, поряд із передбаченими в Регламенті ЄС 2016/679. Крім того, користувачам надано можливість внесення змін до персональних даних та акаунтів.

У зв’язку з активним переходом різноманітних сфер життя в інтернет, Б. Кастерс висуває пропозиції щодо закріплення таких цифрових прав, які мають отримати нормативне закріплення: право на офлайн, право не знати, право на

зміну думки, право знати цінність персональних даних, право на чисте цифрове середовище, право на безпечне цифрове середовище.

На погляд Б. Кастерса, в умовах інформаційного суспільства право не знати, тобто право бути необізнаним щодо певної інформації відносно себе, що може сприяти добробуту особи. Чинне законодавство ЄС та держав-членів містить низку положень про обов'язок розкриття інформації. Поряд із правом на доступ до інформації за ст. 15 Регламенту ЄС 2016/679, йому кореспондує обов'язок державних органів надати суб'єктам інформацію на їх запити, із дотриманням принципів законності, справедливості та прозорості обробки персональних даних. На контролера покладається відповідальність за дотримання принципів та засад обробки та обов'язок надати інформацію суб'єкту даних (на запит) про те, яка інформація щодо нього збирається, обробляється, їх цілі та способи.

На відміну від здійснення права доступу до інформації або, як називають у зарубіжній літературу, «право знати» потребує від особи активних дій, звернення до контролера (компанії) за отриманням інформації, а умови здійснення права потребують обізнаності та додаткових роз'яснень щодо отримання таких даних як кредитні рейтинги, очікувана тривалість життя, стан здоров'я, то здійснення права не знати не потребує активної поведінки.

Наразі право не знати стосується переважно результатів медичних досліджень, обумовлених розвитком превентивної медицини [564, с. 3]. В умовах розвитку превентивної медицини [104, с. 117] право не знати має практичне значення в разі виявлення хвороби або схильності до хвороби, яка може бути діагностовано але при сучасному рівні медицини не можна позбутися та вилікувати[869, с. 480]. Право не знати результати генетичних досліджень законодавчо закріплено в деяких державах ЄС, таких як Швейцарія, Австрія та Німеччина.

Так, особа може забажати не знати очікувану тривалість власного життя, генетичні хвороби, результати досліджень свого здоров'я, щоб не жити з цими знаннями. Вочевидь деструктивне знання невідворотне, його не можна

позбутися, тому коли зайва інформації може нести загрозу життю, держава може вжити заходи для забезпечення обмеження впливу небажаної інформації.

Так подекуди бажаність народження первістка сина або інші класові та кастові традиції в державі, можуть призвести до передчасного переривання вагітності жінкою в разі знання майбутньої статі новонародженої дитини. Тому Закон Індії «Про методику планування сім'ї та передродової діагностики» передбачає заборону реклами послуг про визначення статі дитини, надання таких послуг, їх пошук та підбурювання до правопорушення через високу вірогідність переривання вагітності в разі народження дівчинки.

Науковці Р. Чедуік, М. Левітта Д. Шікл та інші зазначають, що права знати так і права залишатися необізнаним тісно пов'язані з ідеями автономії особи [423, с. 40]. Здійснення права не знати можливо застосовувати в ситуаціях прогностичних тестів та прогнозування за результатами аналізу персональних даних та поведінки в мережі «Інтернет».

Такі держави як Австрія [355], Швейцарія [512], ФРН [533] містять у законодавстві норми, які передбачають право особи не знати, не брати до уваги результат генетичного діагностування або вимагати його знищення. Дані норми спираються на ідею, передбачену ч. 2 ст. 10 Конвенції про права людини та біомедичні, що кожна людина має право знайомитися з будь-якими зібраними даними стосовно свого здоров'я. Поряд із цим, необхідно поважати бажання людини не бути поінформованою щодо даної інформації [157]. Означений підхід відповідає принципу поваги до людини, який висловлено в доповіді Консультативного комітету експертів ВООЗ щодо розробки глобальних стандартів управління та нагляду за редагуванням геному людини [868].

Знання інформації про вірогідну можливість та ризик захворювання тяжкою спадковою хворобою тягне обов'язок страхувальника повідомити про це страховика в разі укладеного договору страхування життя для подальшого перегляду умов договору, а на стадії укладення договору повідомити страховика, що неминуче може призвести до відмови від прийняття компанією особи на страхування або підвищення страхового тарифу та розмір платежу. До того ж

страхувальник зобов'язаний розкрити інформацію в разі перенесення тяжких захворювань родичами при укладенні договору страхування життя, що також може призвести до відмови в укладенні договору страхування або призвести до зростання платежу. У будь-якому випадку особа під час оформлення договору страхування життя зобов'язана повідомити про спадкові захворювання в разі, якщо вона володіє такими даними, та звільнена від обов'язку, якщо немає такої інформації.

З метою розвитку превентивних до клінічних, молекулярних та генетичних досліджень фахівці медичної галузі пропонують передбачити в законодавстві обов'язок роботодавця забезпечити проведення превентивного дослідження працівників, та зобов'язати страхові компанії укладати договори страхування за умови проведення превентивного дослідження.

Означена пропозиція носить дискримінаційний характер як працівників, так і осіб, бажаючих укласти договір страхування життя. Для недопущення зловживання генетичними технологіями, наразі доцільно доповнити ст. 99 Закон України «Про страхування» [166] положенням про заборону оцінку ризику на основі прогностичного генетичного тесту, заборону страховиків вимагати проходження генетичного тестування та запитувати в застрахованих осіб або родичів надання результатів такого тестування. Аналогічне положення має бути передбачено у ст. 2-1 Кодексу законів про працю України про недопущення дискримінації за генетичною ознакою: заборону вимагати від працівників проведення генетичного тестування, подання його результатів, іншої інформації про генетичні особливості працівника (його родичів), а також використовувати роботодавцем результати прогностичного генетичного тестування.

На підтримку закріплення права не знати висловлювалася Ю. Рейкка ще у 1998 році [759, с. 50]. В інтернеті право не знати отримало своє підґрунтя не лише відносно медичних даних. За твердженням М. Косінскі, Д. Стітуел та Т. Графел, обробка великих масивів чутливих даних дозволяє спрогнозувати низку чутливих властивостей фізичної особи як тривалість життя, вірогідність розлучення, вподобань та схильність до зловживання алкогольними та

наркотичними речовинами, ризик серцево-судинних захворювань та окремих видів онкологічних захворювань [610, с. 5803]. На підставі аналізу профілей Facebook 58 000 користувачів, результатів кількох психометричних тестів та деталей демографічних профілів, науковці продемонструвати, наскільки точно в інтернеті можна спрогнозувати якості та властивості поведінки особи, які є конфіденційними та прагнуть залишати в таємниці.

Технології предикативної аналітики на підставі аналізу великих даних, які використовують торгівельні мережі, дозволяють виявляти стереотипи поведінки на підстави обробки даних про покупки клієнтів. Навіть спрогнозували вагітність своїх клієнтів [645]. Слід констатувати, що подібні дії торгівельних мереж можуть призводити й до негативних наслідків, якщо така подія є небажаною для жінки (підлітка), яка не перебуває у шлюбно-сімейних відносинах. Тож адресна прогнозована розсилка реклами, заснована на аналізі великих даних, порушує право на приватність особи.

М. Косінскі, Д. Стітуел та Т. Графел доводять, що вік, стать, характер занять, освіта та характеристики особи можуть бути передбачені з журналу перегляду сайтів користувача. А на основі даних музичних уподобань, даних профілей соціальних мереж – кількість друзів, щільність мереж дружби або мови, що використовується користувачами, розташування та щільності друзів у соціальній мережі, можна передбачити особисті. Означені дані є доступними розробникам веббраузерів, пошукових систем та соціальних мереж. Можна стверджувати, що деякі з подібних передбачень мають високий рівень приречення або самовиконуваних пророцтв. Так, прогнози результатів голосувань за певну політичну партію можуть вплинути на початковий вільний вибір виборців.

Слід визнати, що будь-які спроби приховати інформацію від людини порушують автономію її волі. Тому необхідно проведення відмежування між непоінформованістю про використання автоматизованих систем при прийнятті рішень відносно особи, (відповідно до ст. 13-15 Регламенту ЄС 2016/679) від

прогнозів, отриманих на підставі обробки персональних даних щодо майбутньої поведінки, стану здоров'я, персональних якостей особи.

За твердженням Б. Кастерса, надати право компаніям проводити прогностичну аналітику та не надати особам право не знати про такі результати щодо них, є складним та дискусійним, адже такі дані згодом можуть бути використані для створення системи соціальних рейтингів, кредитів, профілювання, стати підставою для прийняття доленосних рішень, вплинути на життя особи (відмова в надання кредиту, прийняття на роботу тощо). На погляд Б. Кастерса, з права не знати слідує право на вчинення помилки та права на зміну думки.

Підсумовуючи викладене, слід визнати, що під гаслом боротьби з суб'єктивністю, бюрократією, з метою ефективного прийняття рішень розширюються сфери застосування автоматизованих та наполовину автоматизованих систем, які поступово замінюють людину не лише в рутинних діях, а й у прийняті юридично значущих рішень. Постає питання, чи здатний алгоритм об'єктивно та справедливо оцінювати людські долі та приймати морально значущі рішення.

Така, експансія автоматизованих систем актуалізує розвиток цифрових прав, гарантій, спрямованих на захист та недопущення дискримінації людини поряд із могутніми технологіями. Вирішення проблем упереджень має проводитись за допомогою технічних та правових засобів. Запровадження стандартизації та розробка етичних принципів, які дозволять встановити межі справедливого застосування ШІ під час прийняття рішень міжнародними установами, може стати таким засобами. Перед правом постає провідне завдання – створення оптимального балансу між розвитком технологій та нагальною необхідністю збереження контролю людини над ними, поєднанням людського розуму та штучного інтелекту, що постійно розвивається.

3.4. Основні положення про дієздатність фізичної особи у відносинах в мережі «Інтернет»

У мережі «Інтернет» здійснення дієздатності фізичної особи, таких її елементів як правочиноздатність, трансдієздатність, бізнесдієздатність, вимагає проведення реєстрації та створення профілю (акаунта) на відповідній платформі та інформаційно-комунікаційній системі.

Укладення правочинів (купівля-продаж, замовлення робіт та послуг) в мережі «Інтернет» відбувається із застосуванням цифрового профілю. Для проведення автоматичних транзакцій та платежів, користувачі залишають банківські дані у профілях (акаунтах), відповідно до налаштування профілю. Наразі в мережі «Інтернет» фізичні особи, за допомогою цифрових профілів, реалізовують свої права, оприлюднюють результати своєї творчої діяльності та виражають себе. Як було з'ясовано, відповідно до вимог користувацьких угод, компанії залишають певні права суб'єктам створювати профілі під псевдонімом, які не співпадають із фізичною особою. З огляду на тенденцію автентичних акаунтів, цифрові профілі презентують фізичну особу в мережі, а на випадок смерті GAFAM дозволяє перевести статус акаунта в пам'ятний, що є поступовим кроком до майже незалежного існування профілю мережі. Прибічниками антиутопічних сценаріїв висуваються припущення, що з розвитком технологій машинного навчання, цифровий профіль (акаунт) зможе відокремитися від фізичної особи та самостійно виконувати дії, набувати права та обов'язки, укладати правочини автономно, що не в інтересах фізичної особи, творця. Відповідно до антиутопічних сценаріїв, профіль фізичної особи або автоматизованої системи зможе набути від початку обмежену самостійність та згодом, абсолютну самостійність, відокремившись від фізичної особи. Слід визнати посилення конкуренції між автоматизованими системами та людиною [501]. Водночас зазначені побоювання відносяться лише до гіпотетичних ризиків, які несе розвиток ШІ [314], тому актуальним є питання особливостей здійснення представництва (трансдієздатності) в мережі «Інтернет».

Трансдієздатність фізичної особи в мережі «Інтернет» уявляється як здатність обирати представника та виступати представником, здатність своїми діями створювати для інших суб'єктів права та обов'язки, приймати на себе права й обов'язки, що виникають внаслідок дій інших осіб у мережі, а й є питання правового статусу автономного програмного забезпечення – штучного інтелекту.

З погляду Я. Коксвіка, за цифровим профілем (акаунтом) майже завжди ховається фізична особа як оператор. Наразі правильно налагоджена програма, здатна забезпечити виконання одноманітних та автономних задач, обирати контент, сприяти узгодженню умов та укладенню договорів. У мережі агенти, згенеровані штучним інтелектом, представлені профайлом. На думку науковця, віртуальні особи в мережі живуть «віртуальне життя», що актуалізує питання відповідальних осіб за вчинки інтелектуальних агентів, які ладні діяти самостійно та автономно в мережі [842, с. 78]. Твердження науковця щодо вчинення самостійних та автономних дій агентом на сьогоднішньому етапі розвитку автоматизованих систем складно говорити, адже програма виконує саме ті дії, на які її налаштовує (уповноважує) її користувач.

Слід зазначити, що електронний (інтелектуальний) агент являє собою сервісно-орієнтований додаток, який надає користувачам (замовникам) пакет програмного забезпечення, та який діє від імені та за рахунок принципала. Тож фактично нівелюється уявлення про агента як суб'єкта, який володіє визначеними вольовими ознаками. Під терміном «агент» – (від лат. «agere», «діяти» або «працювати) розуміється особа, яка діє від імені або замість іншої особи за її дорученням, представник [644].

Як електронні агенти, так і «традиційні» агентські відносини цілеспрямовані на досягнення мети, поставленої власником (принципалом), водночас характерною властивістю електронного агента є те, що він є програмою, а не фізичною особою, яка діє від імені та за рахунок принципала. Відтак концепція електронного агента фактично нівелює традиційне розуміння агента як суб'єкта, який володіє певними вольовими ознаками.

Слід зазначити, що в науці відсутня єдність точок зору на розуміння електронного агента. М. Овермарс визначає програмного агента (software agent) як систему, здатну автоматично діяти в певному середовищі для досягнення певної мети [729, с. 45]. Б. Сукман визначає електронного агента як комп'ютерну програму або електронний засіб, який використовується для вчинення дій, надання відповідей на електронні документи, автономно або за участі особи [799, с. 25].

У комп'ютерній науці під інтелектуальним агентом розглядається програма, здатна самостійно виконувати дії, задані користувачем комп'ютера без втручання людини, якому притаманні функції: автономності, адаптованості, координації, використання для допомоги оператору або для збору інформації. Автономність інтелектуального агента означає здатність виконувати завдання без зовнішнього втручання з боку людини або іншого програмного забезпечення; адаптованість інтелектуального агента означає здатність сприймати і адаптуватися до зовнішнього середовища і самонавчання; координація означає здатність декількох агентів виконувати завдання разом[188, с. 181]. Прикладами інтелектуальних агентів є комп'ютерні віруси, боти, пошукові роботи, які можуть виконувати збір та постійний пошук необхідної інформації в інтернеті. Агенти функціонують на основі прогам штучного інтелекту, машинного навчання та обробки мови, передбачення поведінки та дій суб'єктів даних за запитами, навіть вчинення протиправних дій. Користувач може дати доручення електронному агенту знайти певну інформацію, вводячи запит у пошуковій системі, а програма опрацьовує запит та надає варіанти, які найбільше відповідають запиту [670, с. 5]. Наразі подібні агенти обмежені налаштуванням алгоритму, а «інтелектуальність» характеризує здатність агентів до пристосовування та навчання [130, с. 157]. Прикладами інтелектуальних програмних агентів є: агенти-боти, які збирають дані про товари, послуги в інтересах користувачів; користувацькі агенти, які вчиняють одноманітні дії в інтересах та на користь користувача (обробляють та сортують листи, пошту, заповнюють форми на сторінках, відправляють відповіді на запити в межах

корпоративної комп'ютерної мережі); предикативні агенти, які здійснюють моніторинг та спостереження за об'єктом, прогнозуючи зміну поведінки (спостерігають за наявністю запасів на товарному складі, дотриманням стану правопорядку); агенти, які збирають, обробляють великі бази даних з метою їх систематизації.

Серед найбільш відомих програмних агентів слід назвати Siri, Cortana, Google Assistant, які обробляють дані користувачів, та IVA, яка аналізує перспективні об'єкти для інвестиційної діяльності та новини у фінансовій сфері [887].

Інтелектуальні програмні агенти, за своєю суттю, є одним із видів автоматизованих систем, створених для досягнення поставлених задач та здатних до самонавчання.

Розробка інтелектуальних автоматизованих систем, покликаних допомагати у виконанні одноманітних, рутинних дій, збирати та обробляти великі масиві даних, відбувається давно. За визначенням С. Рассела та П. Норвига, розробка автоматизованих роботів та систем такими провідними закладами як MIT, Університетом Карнегі-Меллона, Стенфордський університет, IBM сягає 1950-х років [777, с. 31].

У порівнянні з агентом у фізичному світі, для уповноваження якого необхідно видання довіреності від імені принципала, електронного агента уповноважують до вчинення певних дій – електронні команди. Принципалом може бути не лише користувач (фізична особа), а й юридична особа.

Поведінка та вчинки інтелектуальних агентів (характер, необхідний період часу для виконання завдань) може змінюватися завдяки навчанню та впливу інших агентів, наприклад, агент, який невдало уклав кілька договорів купівлі-продажу, змінить свою поведінку наступного разу, звернувшись за допомогою інших агентів. Передбачається, що інтелектуальний агент буде здатний знайти найкращу угоду для клієнта, яку потім автоматично виконає від імені клієнта. Вебботи, будучи віртуальними помічниками, направляють користувача в інтернеті подібно до програмних помічників, навіть набувають певних рис

індивідуальності, перетворюючись у персонажів по мірі взаємодії з користувачами. Боти дозволяють створювати привабливу віртуальну особистість, яка покликана допомогти користувачу у виконанні різноманітних завдань, навіть представляти політичного діяча, відповідати на запитання виборців та планувати участь у майбутніх виборчих перегонах [848].

Як зазначає Ф. Джонсон-Лерд, у результаті навчання система приймає рішення на підставі власних дій та інструкцій, які в результаті мають призвести до здатності проявляти (принаймні, здаватися такими) людські когнітивні процеси та виражати свободу волю. Ці процеси включають формування наміру, прийняття рішень або розірвання домовленості [741, с. 353]. Означена теза випливає з розробок в галузі штучного інтелекту, де споживачі делегують комп'ютерам виконання все більшого кола повноважень, що дає їм змогу швидко виконувати складні завдання та приймати автономні рішення.

У науці висловлюються різноманітні точки зори стосовно статусу автономних систем або ШІ, від статусу об'єкта права до статусу юридичної особи або, навіть, наділення правосуб'єктністю із повним обсягом прав та обов'язків.

Е. Вайценбек називає такі варіанти правового регулювання інтелектуальних комп'ютерних агентів: наділення агентів статусом юридичної особи; визнання за агентами статусу об'єкта права або інструменту комунікації; застосування конструкції агентського договору стосовно інтелектуальних агентів; застосування спеціальної правосуб'єктності електронної особи в межах агентських відносин [859, с. 205].

Я. Коксвік у 2007 році зазначав, що юридична кваліфікація контрактів, що укладаються за участю інтелектуальних агентів залишається невизначеною, і що існуючі норми договірного права не передбачають врегулювання подібних відносини (щодо отримання акцепту у відповідь на пропозицію, яка призводить до укладання договору) [842, с.78].

Відтак до правовідносин за участі з інтелектуальним електронним агентом доцільно застосування конструкції агентського договору та положення

законодавства про агентський договір (ст.ст. 295 ГК, 297 ГК України), коли права та обов'язки за договором, укладеним з третьою особою за дорученням та в інтересах принципала, породжують майнові наслідки для принципала, а не для агента. Відтак агент у результаті укладення агентського договору з принципалом, бере на себе зобов'язання здійснювати в інтересах другої сторони (принципала) юридичні та/або фактичні дії від свого імені або від імені (другої сторони) принципала. Програма, виступаючи в ролі електронного агента, будучи запрограмованою на вчинення певних дій та виконання певних обов'язків діє від імені, в інтересах та за рахунок принципала. З цього слідує, що відповідальним за дії програми – електронного агента витупає принципал, навіть якщо такі дії настали внаслідок несправності програми.

У 1998 році С. Смед, порівнюючи програмних агентів першого та другого покоління зазначив, що на відміну від першого покоління, програмні агенти другого покоління здатні самостійно знаходити джерела інформації та брати на себе зобов'язання, навіть вчиняти несанкціоновані вчинки, які можуть завдавати шкоду. Наприклад, інтелектуальний програмний агент зможе вести особисті справи, торгувати цінними паперами, управляти банківськими рахунками, спочатку діючи в межах наданих користувачем повноважень та по мірі навчання та взаємодії з іншими користувачами і агентами, та покладання більшого обсягу повноважень високо ризикового характеру, інвестування, агенти зможуть укладати правочини за межами наданих повноважень принципала, навіть незаконні правочини. Тож виникає питання щодо особи відповідальної за завдану шкоду та можливості покладання відповідальності на інтелектуального програмного агента [791]. Поряд із особою відповідальною за завдану шкоду, постає питання вибору законодавства, яке має застосовуватися до правовідносин за участі інтелектуальних агентів останнього покоління. У цьому сенсі до виникаючих відносин можуть застосовуватися правові норми про агентські відносини, коли ліцензіат програмного забезпечення встановлює та запускає програму, тож відносини за участі інтелектуальних агентів мають регулюватись агентським законодавством.

Значущість цих питань ілюструє твердження Європейського парламенту, що міститься у звіті від 27.01.2017 з рекомендаціями для Європейської комісії з цивільно-правового регулювання робототехніки, що по мірі поступового розширення автономії роботів, зростає їх функціональність. Стає дедалі складно вважати їх звичайним інструментом у руках фізичних осіб (розробників, операторів, користувачів), що, у свою чергу, актуалізує питання їх правового статусу [493].

Властивості самостійності та автономності інтелектуальних агентів називають С. Бреннер [348, с. 88], Ст. Веттіг, Е. Цехенднер [863], Е. Вайценбек та ін. С. Смед стверджує, що правове регулювання відносин за участі програмних агентів останніх поколінь може бути викликом для права, у зв'язку з високим рівнем автономності машин, та висуває припущення про здатність інтелектуальних агентів приймати автономні рішення без участі фізичної особи по мірі навчання та накопичення досвіду [791].

Можна навести приклади судової практики США, які містять окремі справи притягнення до відповідальності за автономні вчинки машин та програмного забезпечення. У справі McEvens v. Citibank, 1978 року суд визнав банк відповідальним за втрату фінансових коштів під час проведення операції банкоматом, через відсутність технічних можливостей підтвердження вчинення кожної дії, як це було б під час проведення операцій фізичною особою [433]. У справі State Farm Mutual Automobile Company v. Alfred E. Bockhorst, 1972 року страхова компанія була визнана винною та зобов'язана виплатити страхове відшкодування страхувальнику за страховим випадком, який настав після спливу строку договору страхування, через технічну помилку програми. Суд визнав програму уповноваженою стороною (агентом) вчинити від імені та за рахунок страхової компанії певні юридичні дії [410]. У справі Michael A. Clausen v. Beneficial Finance Coompany, 1976 року було встановлено, що банк не виконав вимог закону про кредитування, оскільки згенероване комп'ютером роз'яснення умов виконання договору кредиту, підготовлене програмою без участі фізичної

особи, не надало належної відповіді на питання позичальника та було не ясним для належного виконання [394].

Вищезазначені приклади є свідченням, що суди США розглядають програми як інтелектуальних агентів, а фінансові установи – довірителями, за чий рахунок та в інтересах діє повірений. С. Смед стверджує, суди можуть розглядати програмне забезпечення як учасників відносин. Науковець вважає, що розширюючи попередні підходи судів щодо дій, які вчиняються автономними програмними агентами, останні можуть розглядатися як уповноважені агенти на вчинення юридичних дій від імені та за рахунок принципала. У разі завдання шкоди неправомірними діями чи бездіяльністю агента третім особам, мають застосовуватися положення норм деліктного права, покладення субсидіарної відповідності на принципала за дії агента та розробника програмного забезпечення. З погляду С. Смеда, в разі визнання за інтелектуальними програмними агентами правового статусу у формуванні агентських відносин, відповідальність за дії програмних агентів може бути покладена на ліцензіатів або користувачів як осіб, які набули прав використання виключними правами на об’єкт (програму). Ліцензіати (користувачі), які завантажили програму інтелектуального агента, будуть виступати як принципали в агентських відносинах. Тому відшкодування шкоди, завданої третім особам неправовірними діями чи бездіяльністю інтелектуальних програмних агентів, має покладатися на ліцензіатів або користувачів.

З цього приводу Дж. Фішер зазначає, що автономний електронний агент, здатний укладати правочини без будь-якого втручання фізичної особи, аналогічно тому, як виконує юридичні дії уповноважений агент – фізична особа. За загальним правилом, підставами виникнення агентських відносин є: надання повноважень агенту на вчинення дій, суб’єктом на підставі договору, та схвалення суб’єктом угод вчинюваних в інтересах суб’єкта. На думку Фішера, оскільки для виникнення договірних відносин між принципалом та агентом необхідно досягнення згоди за всіма істотними умовам договору, а щодо відносин інтелектуальних комп’ютерних агентів та фізичної особи, виконання

такої умови як досягнення згоди є неможливим для задоволення цього критерію, може бути застосована юридична фікція згоди сторін [517, с. 540].

Враховуючи вищезазначене, у випадках, коли користувачі (ліцензіати) завантажують та активують програму автономного інтелектуального агента, має застосовуватися законодавство про агентські відносини. На користувачів, як на принципалів в агентських відносинах покладаються обов'язки та відповідальність за шкоду, заподіяну інтелектуальним програмним агентом. Відповідальність за дії інтелектуальних програмних агентів має покладатися на користувачів (ліцензіатів як осіб, які набули використання виключними правами на об'єкт) у договірних відносинах (коли дії агента зобов'язують принципала перед третіми особами). У разі завдання шкоди програмним агентом та виникнення деліктних правовідносин, відповідальність за дії агента поряд із принципалом може покладатися субсидіарно на розробника та страхову компанію. Страховик буде зобов'язаний відшкодовувати шкоду в межах передбачених договором страхування відповідальності за шкоду, завдану третім особам.

Слід навести погляди Ст. Веттіга та Е. Цехенднера, які пропонують застосовування концепції договірної правоздатності у відносинах між інтелектуальним агентом та принципалом [863]. Так, у римському праві раби не володіли правоздатністю, але могли вчиняти дії, які вважалися вчиненими від імені та в інтересах власника або голови сімейства. В. Занкл висловлює позицію наділення електронних агентів не лише правочиноздатністю, а в тому числі правоздатністю та дієздатністю. Така точка зору обґрунтовується тим, що набуття здатності своїми діями вчиняти правочини, має опосередковуватися набуттям правоздатності та дієздатності, оскільки набуття здатності самостійно вчиняти правочини, потребує наділення здатності нести майнову відповідальність у разі завдання шкоди [881, с. 50].

Дослідження питань, пов'язаних зі статусом та правовим регулюванням програмних інтелектуальних агентів, неминуче актуалізує питання правосуб'єктності автоматизованих систем ШІ.

Е. Вайценбек розмірковує щодо питання доцільності наділення інтелектуальних агентів правосуб'єктністю та залишення за ними інструментального статусу засобу комунікації [859, с. 210].

На погляд Б. Гудмана, С. Флаксмена, аргументом на користь визнання певної самостійності за автономними системами є ст. 22 Регламенту ЄС 2016/679, яка передбачає застосування автоматизованих систем під час прийняття рішення [541]. Відносно даного твердження, як вже було доведено в попередньому розділі дисертації, ст. 22 Регламенту ЄС 2016/679 дійсно не виключає можливості застосування автоматизованих систем, але за умови, що остаточне ухвалення рішення, яке несе юридично значущі наслідки, ухвалюється фізичною особою. Тож рішення, які не несуть юридично значущих наслідків, можуть ухвалюватися системою автономно та самостійно.

Т. Кім та Б. Рутледж завертають увагу на алгоритмічну підзвітність компаній перед суб'єктами даних, обов'язку контролера повідомляти уповноважені органи та суб'єктів даних про порушення безпеки даних, та проводити оцінку впливу обробки даних на суб'єктів даних [595, с. 20; 596].

За твердження В. Аль-Маджіда, для наділення інтелектуальних агентів правосуб'єктністю, необхідно визнання за ними права власності на об'єкти, які мають економічну цінність у фізичному світі. Науковець розмірковує щодо можливості набуття інтелектуальними агентами прав на цифрові об'єкти, шляхом заволодіння рахунками, даними кредитних карток тощо. Науковець приходить до висновку, що по мірі зростання автономності, мобільності та здібностей інтелектуальних агентів, за ними може бути визнано право власності на цифрові об'єкти в мережі [306].

Щодо властивостей інтелектуальних агентів, які дозоляють їх відмежувати від решти програмного забезпечення, Ст. Веттіг, Е. Цехенднер називають реактивність (здатність сприймати навколишнє середовище і реагувати на зміни, що відбуваються); проактивність (здатність ініціювати поведінку, спрямовану на досягнення мети); автономність (здатність діяти без прямого втручання фізичної особи, певною мірою контролювати власні дії та функціональність); соціальні

здібності (здатність взаємодіяти з іншими програмними агентами або фізичними особами); адаптивність поведінки (здатність підлаштовуватися під звички, методи роботи та вподобання користувача); мобільність (здатність переміщатися в цифровому середовищі) [863].

Поряд із вищезазначеними властивостями інтелектуальних агентів, М. Вулдрідж та Н. Дженнінгс звертає особливу увагу на такі властивості: мобільність (здатність агента переміщення в мережі); достовірність (припущення, що агент свідомо не повідомляє викривлені або недостовірні дані); доброзичливість (припущення, що агент не переслідує мети введення в оману та нанесення шкоди); раціональність (припущення, що агент діє з метою досягнення поставлених перед ним завдань у спосіб, що не перешкоджає їх досягненню [874].

С. Веттіг та Е. Цехенднер пропонують відмежовувати стаціонарних та мобільних агентів, та стверджують, що з появою мобільних інтелектуальних агентів право розглядає дії програми (комп'ютера) як дії, вчинені оператором. Проте програма інтелектуального агента перебуває не в комп'ютерній системі власника (розробника) програмного забезпечення та інтелектуального агента, а на пристроях користувача. Така властивість агента називається – «мобільністю». «Мобільність» інтелектуальних агентів, обмовлена тим, що розробник мобільного інтелектуального агента (програмного забезпечення) не впливає на функціонування комп'ютерної системи користувача та вчинювані дії інтелектуальним агентом, знаходиться поза контролем розробника. Високий рівень незалежності, просторова віддаленість від користувача по відношенню до розробника, називаються в якості аргументів на користь визнання за інтелектуальними агентами правосуб'єктності. Науковці пропонують створення реєстру автономних інтелектуальних агентів. Для впорядкованого існування високоавтономних та самостійних програм штучного інтелекту, пропонується застосування концепції електронної особи.

На користь обов'язкового запровадження реєстру високоавтономних та самостійних інтелектуальних агентів, електронних осіб також висловлюється Е. Швайнгофер [785, с. 45].

Солідаризуються з позицією створення реєстру автономних самостійних інтелектуальних агентів, з метою їх обліку та належної ідентифікації Т. Ален, Р. Уіддісон та К. Карнов [307, с. 27; 593, с. 161].

Е. Вайценбек аналізує автономність електронних агентів як здатність діяти без прямого втручання фізичної особи чи інших агентів, та здатність контролювати власні дії відповідно до поставленої мети і завдань розробника [859, с. 210].

З погляду С. Рассела та П. Норвига, поведінка агента ґрунтується на його власному досвіді, знаннях (даних, на яких навчалась система та які використовувалися при створенні агента), встановленої розробниками мети та середовища функціонування. Ступінь автономності системи зумовлюється даними, які були використані для навчання та здібностями до навчання [777, с. 31].

Т. Ален та Р. Уіддісон підкреслюють властивість автономності функціонування агентів завдяки здатності до самонавчання. Науковці пропонують розглядати статус інтелектуальних систем з урахуванням ступеня автономності та рівня розвитку: як суб'єкта права або матеріального об'єкта. У випадку визнання за інтелектуальними агентами статусу засобу комунікації, слід застосовувати юридичну фікцію, за якою все те, що походить від агента (програми) визнається таким, що походить безпосередньо від фізичної особи – принципала. Отже, електронний агент має розглядатися як інструмент, телефон, факс. У даній ситуації науковці стверджують, що саме фізична особа, будучи принципалом, укладає договір за допомогою засобів зв'язку, несе відповідальність за власне волевиявлення, інтелектуальний агент виступає в ролі інструменту та не наділений здатністю укладати договори автоматично або від імені, в інтересах принципала. З урахуванням ступеня розвитку технологій,

науковці припускають визнання за інтелектуальними агентами статусу суб'єкта права – юридичної особи, окремої й електронної особи [307, с. 43].

К. Карнов [593, с. 161], А. Дамато та С. Чопра [311, с. 2162; 429] солідаризується з позиціє застосування концепції індивідуального суб'єкта по відношенню до окремих інтелектуальних агентів. Визнання правосуб'єктності за автономними високоінтелектуальними агентами означає, що такий агент може мати майнові права, а також нести відповідальність за дії чи бездіяльність за недбалістю, як фізична особа.

Х. Ейденмулером, Л. Вейном вважають, що на певному етапі розвитку техніки за інтелектуальними системами неминуче буде визнана правосуб'єктність [497, с. 5; 858, с. 107].

С. Веттіг та Е. Цехенднер висловлюються на користь конструкції електронної особи по відношенню до автоматизованих систем, у тому числі електронних агентів, та пропонують запровадження ведення реєстрів агентів онлайн, аналогічно реєстру юридичних осіб. Для реєстрації в реєстрі агентів власник зобов'язаний внести відповідний збір. З урахуванням традиційних підходів про покладення відповідальності за вчинки агента на його власника, розробника програмного забезпечення, науковці замислюється над концепцією спеціальної відповідальні за вчинки інтелектуального агента. Зрештою приходять до висновку, що в разі покладення відповідальності на електронного агента та пред'явлення до нього позову, відповідальність буде покладено на власника інтелектуального агента. Науковці приходять до висновку, що концепція електронної особи повинна мати вирішальну перевагу над іншими підходами та дозволити обмежити відповідальність розробника агента, а запровадження електронного реєстру агентів має забезпечити певний рівень прозорості. Так, контрагент, що планує укласти договір та веде переговори з електронним агентом, зможе перевіряти надійність агентів у реєстрі. Така ситуація має створити умови прозорості технології та може значною мірою підвищити довіру до інтелектуальних агентів [863].

З урахуванням ідеї наділення правосуб'єктивністю електронного агента, Е. Вайценбек досліджує засоби ідентифікації інтелектуальних агентів. Науковець відзначає існування проблемних питань, обмовлених тим, що програмне забезпечення знаходиться на комп'ютерних серверах суб'єктів по всьому світу, обслуговується різними особами та програмний код поширюється на умовах вільних ліцензій [859, с. 206].

І.В. Давидова, С. Журило, В. М. Зубар, І.М. Іліопол звертають авагу, що під час вирішення питання наділення агента штучного інтелекту правосуб'єктністю має враховуватися такий чинник як ступінь автономності інтелектуальних систем та рівень їх розвитку [455, с. 90; 458, с. 487].

Тому визнання правосуб'єктності за інтелектуальними програмними агентами ставить виклики щодо визначення моменту виникнення правосуб'єктності, обсягу прав та обов'язків, виду та заходів юридичної відповідальності за неправомірні діяння, завдані агентом.

Такі дослідники як Р. Кало [363, с. 515], О.Е. Радутний [758, с. 132]. пропонують розглядати «контекстуальний» варіативний правовий статус ШІ, відповідно до якого він може виступати як об'єктом, так і суб'єктом залежно від характеру правовідносин. З урахуванням потужного розвитку технологій та ускладнення правовідносин такий підхід підтримує Дж. Балкіним, [321; 322].

Існують пропозиції щодо ототожнення правового статусу автономної системи та людини, якої дотримується Є. Ціммерман [886, с. 22]. Дана позиція є найбільш спірною та в юридичній науці не находить підтримки.

Поряд із вищевикладеними позиціями, поширеною є точка зору про визнання штучного інтелекту або автономних програмних систем як традиційного об'єкта права, річчю, через відсутність належного обґрунтування та умов визнання за ним правосуб'єктності. Інструментального підходу дотримується С.Д. Хасслер [549], С.М. Солайман [795, с. 155].

Інструментальний підхід стосовно програм та визнання за автоматизованими ШІ статусу об'єкта майнових прав обґрунтовується в галузі права інтелектуальної власності: Г.В. Лебедєвою [96, с. 15], К.Г. Некіт, В.М.

Зубарем [689, с. 240]. Солідаризуючись з даною позицією, що у сфері інтелектуальної власності інструментальний підхід забезпечує розробниками отримання економічного ефекту та забезпечує належний захист результатів творчості [226, с. 150; 243, с. 55; 458, с. 490].

Слушно навести справу Тайлера проти Генерального Комісара з патентів та торгових марок, де Верховний Суд Великобританії поставив крапку в питанні правового статусу ШІ та можливості визнання авторства на винаходи за програмою на ім'я Дабус, розробником якої є позивач (фізична особа). Верховний Суд прийняв остаточне рішення, що для отримання патенту та визнання патентних прав заявник повинен бути фізичною особою [412]. Наразі ШІ залишається інструментом у роботі автора та, навіть [19, с. 194], допомагає для виявлення порушень у галузі інтелектуальної власності.

З огляду на рівень творчого вкладу М.А. Лемлі розглядає можливість передачі об'єктів інтелектуальної власності згенерованих програмами до суспільного надбання [632, с. 21]. Як зазначає Л.Р. Майданик, в Україні об'єкти, створені за допомогою автоматизованих інструментів (програм генеративного ШІ), можуть отримати авторсько-правову охорону в частині створеною фізичною особою [30] та за умови відповідності вимогам законодавства про охороноздатність [219, с. 93; 228, с. 35; 238, с.39; 242, с. 62]. Л.Р. Майданик зазначає, що об'єкти авторського права, які були створені за достатньої участі фізичної особи та застосуванням автоматизованих інструментів, можуть отримати охорону [654, с. 145]. Слід визнати дану позицію слушною, з урахуванням появи програмного забезпечення у сфері архітектури, проєктування та дизайну, яке дозволяє автоматизувати одноманітні дії.

Слід визнати, що загалом цифровізація та транскордонне середовище інтернету неминуче ставить виклики для творчості, визначення критеріїв охороноздатності об'єктів авторського права [231, с. 180; 236, с.122; 244, с. 52; 828, с. 454], порушення прав на товарні знаки в мережі [230, с. 142] тощо.

Крім того, слід зазначити, що не лише в юриспруденції точиться дискусія щодо об'єктивації статусу автоматизованих систем, визнання за

інтелектуальними агентами, статусу суб'єкта права або проміжного статусу між інструментом та квазісуб'єктом. Аналогічно в соціології замислюються над питанням здатності інструментів до дії та сформулюються підходи, які наділяють матеріальні об'єкти здатністю до активних дій.

По мірі зростання використання автоматизованих систем у повсякденному житті та передачі вчинення різноманітних дій автоматизованим агентам, тим більше зростають ризики завдання шкоди фізичним особам. Тож актуальними є проблеми відшкодування шкоди, завданої в мережі. Так, А. Ліор доводить точку зору, що в сучасному світі збільшуються загрози завдання шкоди автоматизованими системами, а з тим інтелектуальними агентами. Науковець розглядає програму ШІ крізь призму акторно-мережевої теорії, де ШІ виступають як вузли – агенти, пов'язані зв'язками (відносинами) з принципалом, за яким стоїть фізична особа. Саме на принципала покладається відповідальність за шкоду, завдану ШІ. У разі заподіяння шкоди системою ШІ, мережа (відносини, де він є учасником) складається з безлічі інших «вузлів», пов'язаних із ним за допомогою різних «ребер» (під даним терміном науковець розуміє підстави виникнення правовідносин). А. Ліор називає таку мережу «мережею нещасних випадків». У даному випадку два найбільш значущі «вузли» – це автоматизована система ШІ та особа, якій завдано шкоду, що пов'язані між собою «ребрами», які мають характер відносин відшкодування шкоди. ШІ та особа, якій завдано шкоду, можуть бути пов'язані договірними відносинами спільної діяльності та ін. Характер «ребер» (підстави правовідносин) має братися до уваги під час визначення відносин між «вузлами». «Вузлами» (суб'єктами) мережі нещасних випадків також є розробники програмного забезпечення, правоволодільці, які пов'язані з автоматизованою системою. «Вузли» (суб'єкти) пов'язані між собою спільними задачами та цілями. Відносини між автоматизованою системою ШІ та особою, якій завдано шкоду, «обмежені» мережею, під якою розуміються відносини відшкодування шкоди. Слідуючи позиції А. Ліора, мережа нещасних випадків є обмеженою, що дозволяє їм служити інструментом для встановлення відповідальних осіб за завдану майнову

шкоду, підстав відповідальності та визначення розміру відшкодування. Мережа нещасних випадків не може бути обмежена заздалегідь визначеною кількістю «вузлів» та «ребер».

На погляд А. Ліора, цінність використання теорії мереж у контексті відносин фізичної особи та ШІ полягає у здатності встановити, що за «вузлом» – програмним агентом, ховається фізична особа (принципал), та переконатися, що саме він має бути притягнений до відповідальності за протиправні дії агента. Адже саме принципал контролює та уповноважує програмного агента на вчинення юридичних та фактичних дій від свого імені в інтересах та за свій рахунок. Інтелектуальний агент не володіє власними інтересами. Науковець застережує, що основні побоювання несе надмірна «лояльність» систем ШІ, де агент своїми діями здатний заподіяти шкоду при виконанні дій та завдань, доручених принципалом, навіть якщо останній не міг передбачити настання негативних наслідків. Науковець наголошує, що саме на принципала, за яким стоїть фізична особа, має наставати відповідальність за шкоду, завдану інтелектуальним програмним агентом [641, с.40].

А. Ліора зазначає, що фізична особа може залишатися не обізнаною про те, що вона вступає у відносини із програмним агентом. У зв'язку з віддаленістю відносин між учасниками в мережі, програмний агент може залишатися непрозорим для фізичної особи та в разі завдання йому шкоди, можуть ускладнюватись можливості вжиття превентивних заходів для запобігання настання нещасних випадків та завдання шкоди. Саме на принципала покладається обов'язок вживати заходи запобігання нещасним випадкам та завдання шкоди алгоритмом. До таких заходів слід віднести укладення договору страхування відповідальності за шкоду, завдану програмним агентом. Можна навести висловлювання Дж. Балкіна, що рабин, будучи принципалом Голема, який виступає агентом, вчиняє дії в інтересах свого власника, а тому саме на нього покладено відповідальність за будь-які вчинки та шкоду, завдану Големом [322].

З твердженням А. Ліора, з точки зору теорії мереж, фізична як вузол у мережі інцидентів може розглядатися як суб'єкт, який контролює вчинки програми ШІ, тобто як людину, яка керує агентом – ШІ. Головний вузол –людина має можливість контролювати, направляти і давати вказівки агенту ШІ відповідно до характеру їх взаємовідносин. Таким чином, вона несе відповідальність за дії та завдані збитки свого агента, яким є програма ШІ. Водночас означене створює хибну дистанцію між принципалом та програмою ШІ. Унікальна структура агентських відносин ставить принципала в позицію, коли він дистанціюється від порушника і мережі нещасних випадків, використовуючи програму ШІ як агента. Доктрина respondeat superior, яка передбачає відповідальність сторони за дії своїх агентів, підтверджує здатність принципала запобігати завдання збитків, незважаючи на штучну дистанцію, яку він створив завдяки своїй агентській перевазі. Розгляд відносин за участі агента – програми ШІ, крізь призму мережі дозволяє побачити, що програма, будучи джерелом підвищеної небезпеки здатна завдати значну шкоду фізичній особі, така шкода є непропорційною тій, яку може завдати фізична особа програмі. Відповідальність завжди покладається на суб'єкта, здатного відшкодувати шкоду, нанесену ШІ агентом.

Р.А. Майданик підтримує підхід про застосування до відносин відшкодування шкоди агентами-ШІ норм законодавства про відповідальність за використання джерел підвищеної небезпеки [289; 653, с.152].

Слід зазначити, що введення воєнного стану в Україні, поширення COVID-19 у світі [879] вплинуло на розширення кількості державних послуг, які надаються за допомогою платформи «Дія» [20, С. 92]. Такі виклики та трансформації вплинули на можливість здійснення сімейної дієздатності та укладення шлюбів. З огляду на розвиток електронного урядування та воєнні дії, подання заяв для вступу у шлюб, безпосередньо укладення шлюбу (в тому числі для певних категорій держаних службовців) стало можливо за допомогою використання інформаційно-комунікаційних технологій без необхідності особистої присутності осіб у приміщенні РАЦС [234, с.135]. Поряд із

використанням дистанційних засобів зв'язку, в окремих випадках церемонія укладення шлюбу відбувається в метавсесвітах [329; 532]. З урахуванням таких тенденцій, С.Б. Булеца та І.Е Ревуцька пропонують доповнити статтю 28 СК України положенням про те, що заява про реєстрацію шлюбу може бути подана жінкою та чоловіком особисто через авторизовані платформи, такі як «Дія», а також доповнити положенням статті 33 СК про те, що шлюб може реєструватися не лише у приміщенні органу державної реєстрації актів цивільного стану, а в тому числі онлайн-форматі за допомогою відповідних сервісів (Skype, Facebook тощо) [18, с. 156; 136, с.74]. Таким чином, внесення змін у законодавство щодо подання заяви про вступ у шлюб та укладення шлюбу, в умовах розвитку технологій дозволяє долати віддаленість та позитивно впливає на суспільні відносини.

На підставі вищевикладеного, можна зробити висновок, що інтелектуальні програмні агенти є об'єктами права. Інтелектуальний програмний агент дійсно характеризується певним ступенем автономності, мобільності, яка дозволяє в межах параметрів налаштування виступати засобом взаємодії з суб'єктами права та інтелектуальними агентами з моменту його завантаження (активації) користувачем за відсутності додаткового контролю або нагляду із розробника. Тож будучи інструментом користувача та розробника не здатний виражати власне волевиявлення та самостійно визначати мету. Інтелектуальний агент залишається інструментом, програмним автоматизованим засобом, за допомогою якого реалізовується волевиявлення суб'єкта права, який виступає розробником автоматизованої системи ШІ або користувачем, який здійснює свою діяльність за допомогою інтелектуального агента. Особами, які несуть відповідальність за шкоду, завдану внаслідок використання інтелектуальних програмних агентів, мають розглядатися суб'єкти права – фізичні або юридичні особи.

ВИСНОВКИ

Повноцінне використання інформаційних технологій та участь у відносинах у мережі «Інтернет», авторизація на державних платформах є умовою здійснення прав людини, участі в соціальному, політичному та правовому житті. Впровадження концепції «сервісної держави» та автоматизованих систем прийняття рішень передбачає глобальну трансформацію державного управління суспільством, від традиційної бюрократичної системи до управління із застосуванням інформаційно-комунікативних технологій. Технологізація та цифровізація процесів прийняття юридично значущих рішень, електронних реєстрів, зростання обсягів збору, обробки персональних даних та поширення технологій електронного профайлу (цифрової ідентичності) фізичної особи неминуче ставить виклики перед цивільним правом. Поряд із значною кількістю досліджень, присвячених питанням цифровізації суспільства та впливу новітніх технологій на фізичну особу, залишаються питання, які потребують подальшого дослідження та відповідей. У даному дослідженні, на підставі аналізу законодавчих, доктринальних положень та судової практики, було зроблено переосмислення концепції правосуб'єктності фізичної особи в мережі «Інтернет», з огляду на нові реалії, розглянути права людини, виникнення яких обумовлено цифровізацією та автоматизацією процесів у суспільстві, що дозволило зробити такі висновки та розробити пропозиції.

1. В інтернеті на перший план виходить сутність людини не як біологічної істоти, а як здатність побудови зв'язків, комунікації, впливу своїми діями на інших учасників комунікації та відносини і взаємозалежності, які виникають. У мережі будь-які вчинки (навіть третіх осіб) можуть впливати на здійснення прав та обов'язків фізичної особи у фізичному світі: алгоритми, які обробляють дані щодо соціальних виплат, кредитів, укладення договорів, прийняття на роботу, навіть визнання винуватості у вчиненні правопорушення; треті особи, навіть невідомі, які залишають позитивні або негативні відгуки формуючи цифрову

репутацію. Натомість в інтернеті фізична особа представлена цифровою ідентичністю – системою даних.

На здійснення прав та обов'язків фізичної особи як у фізичному, так і віртуальному світі впливають дії, вчинені іншими особами в мережі «Інтернет», такі як: результати аналізу персональних даних алгоритмами (профілювання), на основі яких приймаються індивідуалізовані доленосні рішення відносно суб'єкта; завантаження та поширення відео, які можуть ставати вірусними, створення фотомемів, завантажені старі фотокартки друзями, новини про особу, в тому числі неактуальні та застарілі, цифрові профілі, під якими ховаються алгоритми або нейронні мережі (блогери), які генерують візуальний та контекстуальний контент, що не відрізняється від створеного людиною тощо.

2. Запропоновано розглядати цифрову ідентичність у вузькому та широкому розумінні. Властивостями цифрової ідентичності у вузькому розумінні є: нематеріальність – є акаунтом та джерелом персональних даних у мережі, які не підлягають зношенню та амортизації; економічна цінність – елементи цифрової ідентичності можуть характеризуватися попитом та пропозицією, відчужуватися та приносити економічну вигоду її власнику; створюються в результаті активних дій фізичної особи для певної мети та складають набір даних про фізичну особу в певній інформаційно- комунікаційній системі, які ідентифікують її у відповідних системах (органах держаної влади та місцевого самоврядування, фінансових установ та організацій, у соціальних мережах тощо), дані можуть автоматично оновлюватися під час їх зміни в інформаційних системах державних органів та установ; залежність та похідний характер від її «творця» фізичної особи (виражає її волю, не виражає власну автономну волю, перебуває в залежності від фізичної особи та не володіє реальною здатністю своїми вольовими фактичними діями самостійно здійснювати цивільні права та виконувати обов'язки); проєктність або множинність обумовлена відносною анонімністю персональних даних для широкого загалу користувачів (постачальники телекомунікаційних послуг отримують доступ до персональних даних користувачів, які можуть бути

передані уповноваженим органам; суверенність – по мірі розвитку технології децентралізованої цифрової ідентичності на платформі блокчейн – фізична особа має отримати можливість управляти та контролювати доступом до персональних даних за допомогою хмарних технологій.

Властивості цифрової ідентичності в широкому розумінні: є системою даних без прив'язки до конкретного акаунта, включає всі дані, які особа залишає в результаті активної та пасивної діяльності, яка не спрямована безпосередньо на розкриття інформації: (персональні дані, створені акаунти та інші дані в мережі, які слугують ідентифікації фізичної особи в мережі «Інтернет»); не включає в себе анонімізовані та псевдоанімізовані дані, які не дозволяють конкретно ідентифікувати особу.

2. Оскільки відгуки, коментарі про якість послуг, товарів та робіт фізичних та юридичних осіб, які залишаються на цифрових сервісах, можуть у поєднанні з іншими ідентифікаторами (посилання на акаунт, ПІБ, фото тощо) ставати персональними даними та виступати складовими елементами цифрової ідентичності, фізичні особи можуть захищати свої права шляхом звернення до юрисдикційних та неюрисдикційних форм захисту: компаній, які надають послуги управління цифровою репутацією, або платформ для здійснення права на забуття (видалення); до суду з позовом про захист від неправдивих висловлювань та їх спростування.

3. Через ризики зловживання правами та створення діпфейків, функціонування та розробка систем, які використовують ШІ, мають відповідати вимогам та стандартам захисту прав споживачів по відношенню до будь-яких товарів та послуг. Розробники систем мають інформувати суб'єктів даних про їх взаємодію із програмою та використання автоматизованих систем у виготовленні товарів, робіт та наданні послуг. Відсутність належного повідомлення (маркування) суб'єкта про взаємодію із автоматизованою системою має визнаватись порушенням етичних правил використання ШІ.

4. Проаналізовані підходи до формування цифрової репутації. У КНР застосування системи соціального кредиту (рейтингу) є централізованим,

відкритим та прозорим для фізичних осіб, є частиною державної політики, інструментом публічного управління, покарання, заохочення та виступає інструментом соціального оцінювання. За результатами застосування соціального кредиту та оцінки вчинених дій, можуть наставати юридично значущі наслідки для фізичної особи. Із прийняттям Акту ЄС про ШІ в ЄС заборонено використання систем соціального рейтингу, оцінки та прогнозування соціальної поведінки фізичних осіб. В ЄС та США формуються рейтинги довіри та системи обліку репутації органів державної влади, фінансових установ та репутація на сервісах та шерингових платформах. Цифрова репутація створюється фрагментарно.

5. Аналіз щодо високонадійних засобів ідентифікації фізичної особи дозволив зробити висновок про те, що постійність та унікальність такої ознаки може мати в основі своїй складові біометричні персональні дані, а саме геномну інформацію (дані ДНК). Поряд із цим, неконтрольований збір та обробка геномних даних, що збираються для проведення молекулярно-генетичної експертизи, в подальшому має наслідки, пов’язані з ризиками втручання у приватне життя та ставить під загрозу втручання та зловживання правами людини, на що звертає увагу у своїх рішеннях ЄСПЛ.

6. На первинних етапах розвитку інформаційно-комунікаційних технологій було поширеним створення профілів під вигаданими іменами та використання псевдонімів. Поточний етап розвитку мережі «Інтернет» характеризується домінуванням цінностей прозорості та відкритості комунікації в соціальних мережах та уникнення використання псевдонімів як умови успішного просування в інтернеті.

7. Дослідження досвіду застосування технологій розподільних, децентралізованих реєстрів дозволив обґрунтувати розвиток концепції суверенної цифрової ідентичності на базі технології Блокчейн як технології, здатної: забезпечити доступ до основного акаунту та інших пов’язаних акаунтів (електронних грошей, криптовалюти, віртуальної власності в іграх, об’єктів інтелектуальної власності, електронних документів після смерті спадкодавця

тощо); знизити ризики масових витоків та порушень, обумовлених зберіганням, обробкою даних на серверах контролерів; надати користувачам право управління, контролю за доступом до персональних даних, децентралізовано, без участі таких третіх осіб (розпорядників реєстрів та ін.). Створення такої цифрової ідентичності має спиратися на ідентичність людини у фізичному світі.

Перевагами технології суверенної цифрової ідентичності на базі технології Блокчейн є: надання суб'єкту доступу до персональних даних у хмарі, обізнаність про масштаби даних, що збираються, обробляються; надання права контролювати доступ до даних певним періодом часу для виконання певної мети та функції; надання можливості відокремити дані користувача від програм, оскільки технологія функціонує «поверх» даних, що зберігаються у хмарі персональних даних; відображає ідею права на перенесення даних, передбачену ст. 20 Регламента ЄС 2016/679 (після отримання даних від контролера та їх зберігання у хмарі персональних даних, дані більше не повинні «мандрувати» до іншого постачальника послуг); надання постачальникам послуг доступу до персональних даних користувачів за попередньою вираженою згодою та на визначених умовах; забезпечення доступу до різних акаунтів, на випадок смерті спадкодавця, яке покликане вирішити проблему розпоряджень залишених на різних платформах, де був зареєстрований користувач за життя (доступ до електронних грошей, криптовалюти, віртуальної власність, об'єктів інтелектуальної власності, електронних документів комерційної цінності тощо).

З урахуванням розвитку технології суверенної ідентичності, аналізу Європейської стратегії для даних, Білої книги ЄС про ШІ, положень Регламенту ЄС 2016/679, обґрунтовано право на цифрову ідентичність як особисте немайнове право, обумовлене розвитком технологій, передбачає право на визнання цифрової ідентичності, право перешкоджати будь-якому спотворенню та посяганню на цифрову ідентичність, яке здатне завдати шкоди фізичній особі.

8. Кроком на шляху формування автентичної ідентичності фізичної особи в інтернеті є визнання 58 державами світу електронних версій українських документів вебпорталу «Дія», що має надати можливість використання

громадянами України електронного відображення інформації, що міститься в документах, передачі електронних копій відповідних документів, отримання публічних послуг за межами України. Для забезпечення даних нововведень передбачається передача даних демографічного реєстру та інших персональних даних громадян України до ЄС, що покликано спростити роботу державних органів, у тому числі органів, уповноважених проводити реєстрацію актів цивільного стану.

У випадку обміну персональними даними між Україною та ЄС, розробка технології автентичної цифрової ідентичності на платформі блокчейн має забезпечити автоматичне оновлення даних під час їх зміни в інформаційних системах державних органів та установ, і надати ДРАЦС та уповноваженим органам реєстрації в інших державах, встановлювати наявність або відсутність перешкод для вступу в законний шлюб та проводити державну реєстрацію шлюбу за допомогою дистанційних засобів зв'язку через інтернет без особистої присутності осіб на церемонії шлюбу.

9. Відмежування категорій «аватар» та «цифрова ідентичність». Під аватаром розуміється об'єкт прав інтелектуальної власності, який є системою статичних та/або динамічних зображень користувача (реальних чи вигаданих, фантазійних), 2D чи 3D моделей, які можуть містити нікнейм користувача (імена або псевдоніми), що відображає його особистість у відповідних віртуальних середовищах і є результатом інтелектуальної творчої діяльності автора. Фізична особа може володіти певною кількістю аватарів, які можуть бути різними в залежності від того, в якій ролі виступає особа у відносинах віртуального середовища. За таких умов, аватар виступає як складова або елемент акаунту та цифрової ідентичності фізичної особи в інтернеті.

10. Обґрунтовано застосовування терміна «цифрові двійники» по відношенню до системи, яка включає: об'єкт спостереження у фізичному світі; його цифрову проєкцію у віртуальному середовищі; датчики (сенсори), функціонування яких опосередковуються інтернетом речей та об'єднані з метою підвищення ефективності обслуговування та прогнозування функціонування

об’єкта (продукту, виробу та ін.). Цифрова проєкція являє собою програмний аналог об’єкта фізичного світу, який моделює внутрішні процеси, технічні характеристики та поведінку об’єкта спостереження, для чого використовуються дані з сенсорів (датчиків), встановлених на об’єкті. Система цифрових двійників складається з: об’єкта спостереження та цифрової проєкції, які пов’язані між собою за допомогою сенсорів (датчиків) IoT, що дозволяють синхронізовувати та порівнювати зміни, які в них відбуваються, виявляючи відхилення від заданої програми.

11. Проаналізовано, що кукі-файли необхідно розділяти залежно від можливості ідентифікувати суб’єкта: такі, що дозволяють ідентифікувати користувача (несуть функцію ідентифікатора та обробляють персональні данні) та такі, що не дозоляють ідентифікувати користувача (використовуються для автоматичного налаштування сторінки). Використання кукі-файлів, які дозволяють ідентифікувати особу, вимагають дотримання вимог законодавства про захист персональних даних щодо належного повідомлення та отримання згоди суб’єкта даних на обробку. Користувацька угода може передбачати застереження, що компанія не використовує кукі-файли, які конкретно ідентифікують суб’єкта даних.

12. З метою недопущення зловживання генетичними технологіями та дотримання прав людини, запропоновано доповнити ст. 99 Закону України «Про страхування» ч. 4 такого змісту:

«забороняється проводити оцінку ризиків на основі результатів прогностичних генетичних тестів, ставити умовою укладення договору страхування – проведення прогностичних генетичних тестів або вимагати проходження, надання результатів прогностичного генетичного тестування страхувальниками, застрахованими особами або родичами».

Для недопущення дискримінації за генетичною ознакою доповнити ст. 2-1 Кодексу законів про працю України ч. 5 такого змісту:

«забороняється вимагати від працівників та кандидатів на зайняття робочого місця (посади) проведення генетичного тестування, подання його

результатів, іншої інформації щодо генетичних особливостей фізичної особи або родичів, у тому числі будь-яке використання роботодавцем результатів прогностичного генетичного тестування фізичної особи та будь-яка дискримінація за генетичними ознаками».

13. Дослідження підходів до правого регулювання інтернету дозволив простежити два підходи: природно-правовий та позитивістський. Позитивістський підхід або закритий підхід до регулювання інтернету та виникненню цифрової правоздатності властиво: контроль за провайдерами та можливість позбавлення доступу до мережі; повна ідентифікація та авторизація користувачів за номером телефону, який пов'язаний із офіційним посвідченням особи; блокування та обмеження доступу користувачів з певних географічних регіонів до контенту КНР; цензурування та обмеження права вираження користувачів; видалення контенту в мережі з перебігом часу; ідеї, що доступ до мережі інтернет, а також доступ до державних адміністративних та фінансових послуг є правом дарованим державою; послідовне закріплення в законодавстві посилення контролю за провайдерами та можливість позбавлення доступу до мережі, обмеження доступу до західних сайтів та сервісів, цензурування та обмеження свободи вираження користувачів та доступу до інформації, а доступ до інтернету будується на ідеї, що він є правом дарованим державою. Західні держави відображають ліберальний (природно-правовий) підхід до правового регулювання інтернету, а у виникненні цифрової правоздатності покладена ідея фундаментального або природного характеру походження прав, обумовлених самою природою людини, її біосоціальною сутністю. Ця властивість слугує засадою для визначення особистих немайнових прав людини як фундаментальних, виникнення яких обумовлено лише природною сутністю людини. Тому доступ до інтернету можна пов'язувати з виникненням правоздатності фізичних осіб лише в демократичних, правових державах, де забезпечуються права людини та користувачі мають (більш- менш вільний) доступ до нього.

14. Позбавлення особи права доступу до інтернету, в тому числі як санкція за вчинене правопорушення та видалення профілю (акаунту) фізичної особи, як свідчить досвід КНР, може бути прирівняний із позбавленням можливості здійснення фундаментальних прав людини. В умовах цифрового суспільства, доступ до будь-яких товарів та послуг (державних, адміністративних, банківських, транспортних послуг, медицини тощо) тісно пов'язаний доступом до інтернету.

15. Аналіз підходів до правого регулювання мережі «Інтернет» (зокрема КНР), дозволив запропонувати розуміння «цифрової смерті», як правової категорії. У широкому значенні термін «цифрова смерть», може застосовуватися для позначення видалення акаунту за життя користувача за його власним волевиявленням у приватній інформаційно-комунікаційній системі, для створення спадкоємцями цифрових меморіалів на знак пошани померлим та смерті фізичної особи зі здійснення її спадкових прав спадкоємцями в мережі. У зв'язку із розвитком електронного урядування та можливістю згенерувати акаунт фізичної особи у певних державних інформаційних системах, використання добровільного видалення акаунтів користувачем може застосовуватися виключно у приватних інформаційних систем. У вузькому значення «цифрова смерть» передбачає отримання доступу до акаунту після фізичної смерті особи для доступу до контенту та здійснення спадкових прав у мережі, який призводить до трансформації цифрової ідентичності та є підставою відкриття спадщини.

Необхідно розмежовувати: добровільне видалення акаунту (на підставі рішення фізичної особи або правонаступників) та примусове видалення акаунту як застосування санкції за вчинене правопорушення за рішенням суду, або порушення умов користувацької угоди за рішенням інтернет-сервісу, яке може призводити до обмеження доступу до товарів та послуг.

16. Із фактом смерті фізичної особи як підставою припинення її цивільної правосуб'єктності пов'язується настання правових наслідків у вигляді відкриття спадщини та права спадкоємців на доступ до залишених даних у вигляді акаунтів

(профілів) у соціальних мережах, криптовалютних біржах, віртуальних іграх та різноманітних сайтах, які можуть мати майнову цінність, інших цифрових об'єктів, які залишилася після смерті спадкодавця. У зв'язку з тим, що внаслідок смерті фізичної особи відбувається правонаступництво, доцільно говорити про трансформацію цифрової ідентичності в силу переходу прав на цифрове майно та отримання уповноваженими особами доступу до акаунту (профілю) в інтернеті.

17. Аналіз існуючих підходів у США та окремих державах ЄС дозволив виокремлювати два напрями правового регулювання доступу до цифрового майна після смерті фізичної особи: перший – визнає тісний зв'язок особи з акаунтом (листуванням, щоденниками, фотокартками тощо), спрямований на забезпечення балансу дотримання особистих немайнових прав та інтересів спадкодавця, та вимагає залишення спеціального розпорядження спадкодавцем для отримання доступу до майна із призначенням особи, (у разі відсутності прямого волевиявлення в заповіті або цифрового розпорядження спадкодавця, платформа надає мінімальний обсяг даних або загалом не надає доступ до акаунту); та другий підхід, який визнає право спадкоємців на доступ до цифрових речей як матеріальних благ та застосовує принципи універсального правонаступництва, за яким права за користувацькою угодою переходять до спадкоємців за законом (Німеччина), якщо в законодавстві не передбачено спеціального порядку спадкування цифрових активів (нехтуючи засадами анонімності, таємниці листування тощо).

18. Для недопущення виникнення суперечок щодо пріоритетності спадкування цифрового майна, в разі залишення цифрового розпорядження на платформі та нотаріально засвідченого заповіту, де спадкоємцями зазначені різні особи, запропоновано доповнити ЦК України положенням про пріоритетність договірного розпорядження над заповітом, складеним на те саме майно, та доповнити ЦК України ст. 1228-1 «Спадкування цифрового майна» наступного змісту:

«1. Заповідач може залишити розпорядження на цифровій платформі або в заповіті, в якому призначити особу, до якої має перейти право власності на цифрове майно в разі його смерті.

2. Договірні розпорядження щодо цифрового майна залишені заповідачем на випадок смерті мають пріоритет над заповітом, складеним на те саме майно.

3. Доступ до особистого листування, щоденників може бути надано спадкоємцям, якщо спадкодавець залишив пряме розпорядження про розкриття таких даних у розпорядженні або заповіті.

4. У разі, якщо спадкодавець не залишив розпорядження щодо цифрового майна в заповіті або на цифровій платформі, спадкування такого майна відбувається відповідно до закону або користувацької угоди».

19. GAFAM та інші технологічні компанії зацікавлені в розвитку цифрових меморіалів, оскільки збір, обробка та аналіз персональних даних померлої особи для навчання програм ШІ не захищається законодавством про захист персональних даних та Регламенту ЄС 2016/679, не поширюється на захист персональних даних померлих осіб. До того користувачі, які відвідують цифрові меморіали, проводячи час в мережі, отримують рекламу, яка власне і є джерелом прибутку GAFAM та решти Інтернет-гігантів.

20. Правосуб'єктність фізичної особи в мережі «Інтернет» складають цифрові права, які можна визначити як різновид прав людини нового покоління, які виражені в цифровому середовищі, реалізуються в межах інформаційно-комунікаційних систем, можуть бути закріплені в законодавстві та відповідних інформаційно-комунікаційних системах, належне виконання яких може бути гарантовано державою та забезпечене інформаційною системою (програмою) автоматично.

Цифрові права не є природними правами, які б походили від природи людини як біологічного виду. До цифрових прав можна віднести як особисті немайнові, так і майнові права, здійснення яких обумовлено існуванням мережі та інформаційно-комунікаційних систем (право вільного доступу до мережі;

право на інформацію та доступ до інтернету; право на приватність у мережі; право на безпеку в мережі; право тощо) зокрема традиційні права, здійснення яких відбувається в мережі.

На можливість здійснення правосуб'єктності фізичної особи впливають не лише такі чинники як громадянство, вік, психічне здоров'я, а в тому числі, й технічні можливості, навички та знання, розвиток нових технологій, доступ до мережі (електроенергії), цифровий розрив.

21. Розглянуті цифрові права, існування яких обумовлено розвитком технологій: право на інформацію про обробку персональних даних та право на доступ до персональних даних; право на уточнення даних; право на видалення даних (право бути забутим); право на обмеження обробки персональних даних; право на перенесення персональних даних; право не бути об'єктом автоматизованого прийняття рішення та право на захист від автоматизованого рішення, яке має правові наслідки; право на заперечення проти обробки персональних даних; право знати механізм автоматизованої обробки персональних даних.

22. Технологічний розвиток послаблює можливість надання згоди суб'єктами даних відповідно до вимог законодавства про захист персональних даних, отримання дійсної законної згоди для кожної мети обробки стає перепоною для розвитку бізнесу, впровадження інновацій та систем ШІ. За допомогою формально виражених дозволених умов обробки даних, суб'єкт даних може повідомляти контролерів про свої наміри щодо обробки даних, вказувати прийнятні цілі обробки, збору, використання даних, передачу третім особам, терміни обробки та ін. Умови (налаштування) приватності мають обиратися суб'єктом при завантаженні додатку на свій пристрій, дозволяючи налаштувати дозволені види обробки, мету та керувати згодою на обробку. Перед початком збору персональних даних контролер має ознайомитися із умовами, дозволеними цілями збору, обробки, умовами передачі третім особам. Результатом порівняння умов допустимого використання персональних даних суб'єктом та умовами збору, обробки даних контролера є досягнення

домовленості між двома сторонами про умови приватності в мережі. Такий підхід має дозволити не лише контролерам, а й суб'єктам даних виражати свої вимоги в забезпеченні контролю та конфіденційності щодо обробки їх персональних даних.

23. Визначення змісту права на інформаційну приватність: право особи контролювати обсяг та зміст інформації, пов'язаної зі збором, обробкою, поширенням та використанням персональних даних; правомочність вимагати від суб'єктів господарювання та органів державної влади виконання їх обов'язків щодо здійснення суб'єктом його правомочності доступу до персональних даних, правомочності на уточнення даних, правомочності видалення даних, правомочності обмеження обробки персональних даних, правомочності перенесення персональних даних; правомочності не бути об'єктом автоматизованого прийняття рішення, правомочності заперечувати проти обробки та обмеження обробки персональних даних, правомочність знати механізм автоматизованої обробки даних; право на захист у разі незаконного збору, обробки, зберігання персональних даних та вимагати застування державно-примусових заходів у випадку порушення суб'єктивного права. Тож кожен випадок здійснення права на інформаційну приватність може бути розглянутий за трьома критеріями і трьома можливостями поведінки.

24. Об'єктивними чинниками, які обумовлюють зміщення балансу недоторканності приватного життя у сторону відкритості та підвищують можливості зовнішнього впливу на приватне життя фізичних осіб: 1) фундаментальні зміни в суспільній свідомості та формування нової системи пріоритетів та цінностей; 2) розвиток інформаційно-комунікаційних технологій, які передбачають можливості дистанційного спостереження за фізичними особами.

25. Проаналізовані технічні та організації заходи, які зобов'язані впроваджувати контролери для забезпечення приватності за замовчуванням та вбудованої приватності, з огляду на рівень наукового та технічного розвитку. Контролери мають приймати до уваги критерій «рівень науково-технічного

розвитку» під час забезпечення заходів безпеки персональних даних до всіх технічних та організаційних заходів з моменту їх отримання. На формування підходів до забезпечення захисту персональних даних та положень Регламенту ЄС 2016/679 вплинули принципи Є. Кавукян.

26. Гарантіями недоторканності приватного життя та захисту персональних даних фізичних осіб у мережі «Інтернет» є: згода суб'єкта на обробку даних та спеціальних категорій даних; обмеження на прийняття юридично значущих рішень із застосуванням автоматизованих систем; обмеження на передачу персональних даних в юрисдикції та держави, які не забезпечують законний збір та належні гарантії обробки персональних даних і прав недоторканності приватного життя; вимоги до технічних засобів захисту персональних даних для запобігання неавторизованого доступу до даних, усунення наслідків їх розкриття; розробка програм та алгоритмів на стадії проєктування з урахуванням вимог захисту персональних даних за призначенням та замовчуванням.

27. Згода на збір та обробку персональних даних, будучи єдиною підставою обробки, яка залежить від рішення особи, залишається провідною юридичною підставою для обробки: даних дітей; чутливих даних; у разі обробки персональних даних для автоматизованого прийняття рішень, профілювання та передачу даних до третьої країни або міжнародної організації. Згода є інструментом захисту права на недоторканність приватного життя та гарантією здійснення прав та свобод у мережі, має відповідати принципам обробки (справедливості, законності та прозорості; цільової обробки; мінімізації даних; точності; цілісності та конфіденційності; обмеженості зберігання).

Поряд із значущістю згоди суб'єкта даних, розвиток автоматизованих систем безперервного збору та обробки персональних даних створює перепони для належного виконання обов'язку контролерів отримати законну згоду на обробку персональних даних, відповідно вимог Регламенту ЄС 2016/679, як вільно надану, усвідомлену для досягнення конкретної мети обробки.

28. Здійснення права суб'єкта даних на доступ до персональних даних має важливе значення, оскільки може бути необхідною умовою здійснення інших прав суб'єктів даних, передбачених законодавством.

З урахуванням правозастосовчої практики членів ЄС, здійснення права на доступ до даних має виключення, обумовлені неможливістю конкретної ідентифікації одержувачів, яким розкривались дані. З метою реалізації цього положення доцільно доповнити частину 1 статті 19 Проєкту Закону України «Про захист персональних даних» від 25.10.2022 № 8153 пунктом 10 такого змісту:

«несанкціоноване розголошення даних та одержувачів даних, за винятком, якщо неможливо ідентифікувати цих одержувачів або якщо запит суб'єкта даних є явно необґрунтованим, або надмірним, контролер може вказати суб'єктам даних лише категорії відповідних отримувачів, не розкриваючи фактичну особу».

29. Встановлено, що законодавство та судова практика ЄС передбачає обмеження здійснення права бути забутим, врівноважуючи інтереси контролерів даних та суб'єктів даних. Контролери можуть відмовити в здійсненні права бути забутим та виконанні запиту суб'єкта даних. Право на забуття не застосовується по відношенню до реєстраційних даних компаній, у разі виникнення колізії між правом на недоторканність приватного життя та забезпеченням прозорості ділових відносин.

30. В умовах інформаційного суспільства, обов'язку контролерів підтримувати актуальність персональних даних, зростає значущість здійснення права суб'єкта на уточнення та надання додаткових даних. З метою успішного здійснення права на уточнення, доповнення неповної інформації в первинних даних або неточності результатів профілювання, в разі включення особи до категорії (профілю), яка не відповідає її здібностям, стану здоров'я, запропоновано ст. 20 Проєкту Закону України «Про захист персональних даних» доповнити ч. 4 такого змісту:

«4. Право суб'єкта персональних даних на виправлення персональних даних передбачає право внесення виправлень у результати профілювання».

31. У результаті поширення використання систем інтелектуального аналізу великих даних, розширюється сфера застосування цифрового профілювання (маркетинг, працевлаштування, відстеження ефективності працівників, судочинство, фінансові та адміністративні послуги, тощо). Дослідження позицій західних науковців дозволили стверджувати, що внаслідок цифрового профілювання створюються нові дані, які не є ідентичними тим, які були надані суб'єктом даних, а метод профілювання може створювати ризики для здійснення прав та свобод людини в демократичному суспільстві, дискримінацію та обмеження права доступу до певних товарів та послуг, підвищувати ризики втручання у сферу приватного життя. Людина може потрапляти в певні категорії, не знаючи про результати.

Проаналізовано, що для пом'якшення наслідків профілювання та недопущення стигматизації в суспільстві, в доктрині висувається ідея права почати все з чистого цифрового аркуша, яке має дозволити суб'єктам розпочати абсолютно нову цифрову ідентичність в умовах цифровізації.

32. Проведений аналіз законодавства та правозастосовчої практики ЄС дозволяє стверджувати, що наслідок «брюссельського ефекту» у сфері захисту прав людини в мережі «Інтернет» проявився в тому, що Регламент ЄС 2016/679 став золотим стандартом правового регулювання інформаційної приватності у всьому світі, та значна кількість держав обрали шлях односторонньої регуляторної глобалізації та слідування вимогам ЄС. Для технологічних компаній США «брюссельський ефект» виявився в тому, що Суд ЄС визнав механізми та керівні принципи передачі за договорами «Безпечної Гавані» та «Щита Приватності», укладених між ЄС та Міністерством торгівлі США такими, що не відповідають стандартам захисту персональних даних ЄС. Технологічні компанії США, які займаються збором та обробкою персональних даних на території ЄС, здійснюють транскордонну передачу даних з ЄС до США, змушені приймати стандартні договірні положення захисту персональних даних

(попередньо схвалені контракти, які забезпечують правове підґрунтя для передачі даних між ЄС та США), або використовувати обов'язкові корпоративні правила (внутрішні правила для передачі персональних даних до території США) відповідно до вимог Регламенту ЄС 2016/679.

33. Встановлено, що залежно від ступеня та якості втручання людини у процес прийняття рішення, розрізняють алгоритмічні системи: повністю автоматизованого прийняття рішень, які не залежать від участі людини та частково автоматизовані з остаточним прийняття рішення людиною.

34. Аналіз правозастосовчої практики та доктрини дозволяє стверджувати, що застосування систем віддаленої біометричної ідентифікації має позитивний вплив у таких сферах як правозастосування, підвищує ефективність роботи правоохоронних та судових органів у галузі боротьби зі злочинністю, водночас технологія несе ризики використання її для масового спостереження. Тому з урахуванням необхідності дотримання справедливого балансу між конкуруючими інтересами осіб у захисті недоторканності приватного життя та публічними інтересами (національної безпеки, запобігання, розслідування, виявлення та переслідування кримінальних злочинів та/або виконання покарань), висловленої позиції Європейського парламенту, потреби створення відповідальних, антропоцентричних та заслуговуючих довіри систем ШІ, розглянуті випадки коли застосування технології несе високі ризики для суб'єктів даних та має бути заборонено.

35. Проаналізовано, що з метою забезпечення прав людини контролери мають право використовувати системи алгоритмів при прийнятті юридично значущих рішень лише у випадках, якщо: необхідно для укладання або виконання договору; дозволено законодавством, що застосовується по відношенню до контролера; суб'єкт даних надав явно виражену згоду на обробку.

Встановлено, що Регламент ЄС 2016/679 забезпечує надійний захист від автоматизованого прийняття рішень, але в нинішньому вигляді цей захист може виявитися неефективним, з огляду на поширення застосування систем

автоматизованого прийняття рішень та автоматизованої обробки даних для підтримки прийняття рішень людиною, що є прогалиною у здійсненні принципів прозорості та підзвітності.

Враховуючи досвід ЄС, доцільно передбачити в законодавстві України право на розкриття логіки прийняття індивідуального рішення по відношенню до конкретного суб'єкта даних, аналізу вхідних даних, статистичного аналізу, перевірки коду (конструкції), визначення чутливості окремих даних (які саме змінні зумовили результат) та обов'язок контролера у разі прийняття рішення із застосуванням алгоритму надати інформацію суб'єкту даних про логіку рішення, що лежить в основі автоматизованої обробки рішення, прийнятого щодо нього. Крім того, суб'єктам даних має бути надано право оскаржувати такі прийняті рішення. З цією метою доцільно доповнити Проєкт Закону України «Про захист персональних даних» від 25.10.2022 № 8153, ст. 25-1 «Право на роз'яснення та оскарження індивідуальних рішень, прийнятих за участі автоматизованих систем» таким змістом:

«1. У разі використання автоматизованої системи при прийнятті рішення, яке має юридично значущі наслідки для суб'єкта персональних даних або іншим чином істотно впливає на нього, суб'єкт персональних даних має право звернутися до контролера для отримання роз'яснення та обґрунтування обставин прийняття індивідуального рішення за участі автоматизованої системи.

2. Суб'єкт персональних даних має право звернутися до контролера для оскарження індивідуального рішення, яке має юридично значущі наслідки або іншим чином істотно впливає на нього до суду, в разі його прийняття автоматизованою системою або за участі автоматизованої системи при прийнятті рішення».

36. Проаналізовані виклики використання автоматизованих систем для здійснення прав людиною: 1) проблема прозорості: (недостатня пояснюваність роботи алгоритмів; незбалансований доступ до інформації; люди не завжди знають, з ким вони взаємодіють: з ШІ, чи з людиною); 2) непрозорість

інформації про потенційні наслідки та відсутність довіри суспільства, через відсутність належної обізнаності про функціонування алгоритму; 3) проблема виявлення достовірних фактів та фейків; 4) упередженості; 5) низький рівень якості даних та відсутність репрезентативності; 6) небезпеки надмірного використання, які охоплюють (застосування ШІ для вирішення завдань, для яких він не застосовуваний, встановлення причинно-наслідкових зв'язків, прогнозування індивідуальних результатів); 7) застосування системи, яке призводить до виникнення вразливостей суб'єктів даних.

37. Встановлено, що законодавство ЄС вимагає від суб'єктів господарювання не приймати рішення стосовно фізичних осіб, які засновані виключно на автоматизованій обробці персональних даних, тобто прийняття рішення системою ШІ. Для того, щоб запобігти такій практиці, на контролера даних, який здійснює профілювання, покладено обов'язок використовувати автоматизовану процедуру спільно з остаточним прийняттям рішення людиною. Контролер зобов'язаний вживати заходи для недопущення прийняття рішення на основі даних про расу, етнічне походження, політичні переконання, релігію, членство у профспілковій організації, генетичних схильностях, стану здоров'я або сексуальної орієнтації. Означене обумовлено технологічною специфікою обробки великих даних, які не передбачають можливість виключити категорію даних із усього масиву інформації, водночас дозволяють не брати до уваги певні дані на етапі їх аналізу та прийняття рішення.

38. Встановлено, що на відміну від ЄС, де діє Регламент ЄС 2016/679, який стосується питань обробки персональних даних, прозорості алгоритмів, поширюється та вимагає дотримання всіма державами членами ЄС, в США відсутнє єдине законодавство на федеральному рівні, яке б регламентувало питання збору та обробки персональних даних, забезпечувало б прозорість та підзвітність алгоритмів. Застосування систем автоматизованого прийняття рішень у США відбувається з урахуванням специфіки кожної ситуації, вимагає дотримання норм антидискримінаційного законодавства, обмеження (заборону)

обробки чутливих персональних даних (стать, расова приналежність тощо) та прийняття на їх основі рішень.

39. У рішенні про використання алгоритму мають бути відображені способи функціонування алгоритму. Водночас у разі законодавчого закріплення вимоги прозорості функціонування систем автоматизованого прийняття рішень постає питання оптимальних шляхів її забезпечення, оскільки робота алгоритму виглядає як математична формула, недоступна для сприйняття пересічними користувачем. До того ж, у разі розкриття всієї логіки функціонування алгоритму, фізична особа зможе маніпулювати даними для отримання певного вигідного для неї результату.

40. Встановлено, що обґрунтування людиною прийнятого рішення алгоритмом або логіки функціонування системи «чорної скриньки», виправдання правдоподібності хибного рішення алгоритму, у разі нехтування особою власним критичним мисленням та надмірною довірою алгоритму, у західних джерелах, пропонується називати алгоритмічним або математичним відмиванням. Математичне відмивання може здійснюватися випадково або цілеспрямовано суб'єктами прийняття рішень.

41. Встановлено, що інтелектуальний програмний агент є об'єктом права, характеризується певним ступенем автономності, мобільності, яка дозволяє в межах параметрів налаштування виступати засобом взаємодії з суб'єктами права та інтелектуальними агентами з моменту його завантаження (активації) користувачем, за відсутності додаткового контролю або нагляду розробника. У разі завдання шкоди програмним агентом та виникнення деліктних правовідносин, відповідальність за дії агента поряд із принципалом може покладатися субсидіарно на розробника та/або страхову компанію.

42. Делегування прийняття юридично значущих рішень алгоритмам поступово та непомітно змінює людське буття. В умовах цифоровізації, зростає відповідальність юристів у збереженні ролі Людини в цифровому світі, де програмний код прагне затьмарити норми права, а технології стають розумнішими ніж людина. Алгоритми мають залишатися виключно

інструментом у руках людини, а роль права – зберегти біологічну людину в новому світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Басиста І.В., Удовенко Ж.В., Кулинич М.-М.А. Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. Науковий вісник Ужгородського Національного Університету, Серія Право. 2024. № 80. Ч. 3. С. 19-38. URL: https://visnyk-juris- uzhnu.com/wp-content/uploads/2024/03/81_part-3.pdf. (дата звернення 26.12.2024).

2. Баловсяк Н. Цифрове безсмертя. Як штучний інтелект експлуатує цифрові копії людей. 3.03.2023. URL: https://tyzhden.ua/tsyfrove-bezsmertia-iak-shtuchnyj-intelekt-ekspluatuie-tsyfrovi-kopii-liudej/ (дата звернення 01.04.2024).

3. Баловсяк Н. Старший брат більше не стежить за тобою. Чому демократичні країни відмовляються від технологій розпізнавання облич. 3.11.2021. URL: https:// chas.news/ future/starshii-brat-bilshe -ne-stezhit-za-toboyu -chomu-demokratichni -kraini-vidmovlyayutsya -vid- tehnologii- rozpiznavannya-oblich (дата звернення 12.03.2022).

4. Балинська О.М. Семіотика права: монографія. Львів: ЛьвДУВС, 2013. 416с.

5. Бауман З. Глобалізація. Видавництво Києво-Могилянська Академія. К. 2008. 112 с.

6. Берназюк Я. Штучний інтелект як основа цифрового судочинства: помічник чи майбутній конкурент судді? *Всеукраїнський семінар для суддів місцевих та апеляційних судів "Застосування штучного інтелекту (artificial intelligence) в правосудді: зарубіжний та вітчизняний досвід"* 12 квітня 2024 року. Національна Школа Суддів Одеське Регіональне Відділення. URL: https:// supreme.court.gov.ua/ userfiles/media/new_folder_for_uploads/ supreme/2024_prezent/artificial_ intelligence_ bernaziuk. pdf__(дата звернення 26.12.2024).

7. Берназюк Я. Штучний інтелект та система правосуддя України: результати співпраці у році, що минув. 07.01.2025. URL:

https://so.supreme.court.gov.ua/authors/934/shtuchnyi-intelekt-ta-systema-pravosuddia-ukrainy-rezultaty-spivpratsi-u-rotsi- sh%D1%81ho-mynuv (дата звернення 30.01.2025).

8. Бідюк П., Бондарчук В. Сучасні методи біометричної ідентифікації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2009. № 1(18). С. 137-146.

9. Біла книга з регулювання ШІ в Україні (версія для консультації) Міністерство цифрової трансформації України. червень 2024. URL: https:// thedigital. gov.ua/storage/ uploads/ files/page/ community/docs/ Регулювання%20ШІ.pdf (дата звернення 01.11. 2024).

10. Білоцький В., Погорілий В., Борис С. Чому діпфейк – злочин і як з ним боротись? 17.06.2021. URL: https:// www.juscutum. com /news/chomu-dipfeyk - zlochin-i-yak-z-nim-borotis-poyasnennya-advokata (дата звернення 26.12.2023).

11. Бінґем Т. Верховенство права. URL: https:// zib.com.ua/ru /161802-the_rule_of_law_ toma_binema_zyavivsya_ukrainskiy_ pereklad.html (дата звернення 26.10.2024).

12. Бригинець С. Біометричні дані: збір і захист у Європі, США та Україні. *Юридична газета.* 2019. № 40 (694). URL: https: //yur- gazeta.com/ publications/practice/inshe/ biometrichni-dani- zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html (дата звернення 26.10.2022).

13. Братасюк О.Б., Ментух Н.Ф. Поняття та класифікація цифрових прав в Україні. *Юридичний науковий журнал.* 2021. № 10. С. 58-61.

14. Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право.* 2020. № 1(32). С. 33-46.

15. Бровінська М. Forbes: ШІ створює порнографічні діпфейки з фото реальних людей, користувачі викладають їх на Reddit, Twitter та Instagram. Як таке можливо? 10.05.2023. URL: https:/ /dev.ua/ news/forbes -shi-stvoriuie-pornohrafichni-dipfeiky-z-fotohrafiiamy-realnykh-liudei-yak- take-mozhlyvo-1684652081?fbclid =IwAR2ZOnhYO _FjFAJw2eeIo5vd Oaia8oc95bf6GnZqsFOQKh0dP6BfWYeeoNI (дата звернення 20.11.2023).

16. Бутнік-Сіверський О.Б. Цифрові та віртуальні активи: методологія, правові аспекти, нематеріальні ресурси. *Теорія і практика інтелектуальної власності.* 2024. № 2. С. 94-104.

17. Булавіна С., Давидова Т. Наслідки недотримання права на приватність у мережі Інтернет: міжнародний аспект. *Історико-правовий часопис*. 2020. № 1 (15). С. 8-13.

18. Булеца С.Б., Ревуцька І.Е. Місце диджиталізації при укладенні шлюбу в Україні. *Електронне наукове видання Аналітично-порівняльне правознавство.* 2023. №5. С. 156-162. URL: http://app- journal.in.ua/ wp-content/uploads/2023/05/28.pdf (дата звернення 28.10.2024).

19. Булеца С.Б. Захист торговельної марки в сфері моди та за допомогою штучного інтелекту. *Аналітично-порівняльне правознавство*. № 2. 2024. С.193-200.

20. Вакулін Р. Перспективи застосування штучного інтелекту в правосудді. *Матеріали конференцій МЦНД* (Полтава, 21 червня 2024 р.). С. 88-90. URL: https://archives.mcnd.org.ua/index.php/conference-proceeding/article/view/23(дата звернення 22.11.2024).

21. Васильченко В. Псевдонім: Імена-маски в Інтернеті. 11.01.2025. URL: https://uain.press/blogs/psevdonim-imena-maski-v-interneti-645649 (дата звернення 01.02.2025).

22. Верлос Н.В. Конституціоналізація цифрових прав людини: вітчизняна практика та зарубіжний досвід. *Часопис київського університету права.* 2020. №2. С. 129-133.

23. Використання електронного підпису як засобу ідентифікації під час користування електронними сервісами 22.07.2021 URL: https://volodarska-gromada.gov.ua/news/1626934605/ (дата звернення 18.10.2022).

24. Віртуальний центр Дія.Бізнес. URL: https:// business. diia.gov. ua/virtual-center-diia-business (дата звернення 16.12.2022).

25. Володавська В. Заборони та свободи в інтернеті: як виглядатиме Декларація цифрових прав людини. 23.05.2019. RL: https://zmina.info

/articles/zaboroni_ ta_svobodi_v _interneti_jiak_vigljiadatime_deklaracijia_cifrovih_prav_ljiudini/ (дата звернення 16.12.2022).

26. Волкова Н.В. Засоби індивідуалізації фізичних осіб (окремі аспекти) *Актуальні проблеми держави та права* 2008. С. 238-243.

27. Волкова Н.В. Цивільно-правові засоби індивідуалізації фізичних осіб. Автореферат дис.канд. юрид. наук. 12.00.03. Одеса, 2008. 18 с.

28. В Україні запускають Єдину системи відеомоніторингу стану публічної безпеки, у тому числі – розпізнавання обличчя. 16 січня 2024. URL: https://sud.ua/uka/news/publication/290740-v-ukraine-zapuskayut-edinuyu-sistemu-videomonitoringa-sostoyaniya-publichnoy-bezopasnosti-v-tom-chisle-raspoznavanie-litsa?fbclid=IwAR0_pXDJx43oMd9pL0JKnbwnAXffs1hAHaWROx9a4HFhjNBob_uxpbe532Y (дата звернення 16.12.2024).

29. В Україні введуть систему відеонагляду за громадянами і звірки їх даних для ідентифікації – у тому числі про місце проживання. 9 вересня 2024. URL: https://sud.ua/uk/news/publication/310121-v-ukraine-vvedut-sistemu-videonablyudeniya-za-grazhdanami-i-sverki-ikh-dannykh-dlya-identifikatsii-v-tom-chisle-o-meste-prozhivaniya (дата звернення 16.11.2024).

30. В Україні вперше зареєстрували авторські права на твори, які містять зображення, згенеровані ШІ. September 24, 2024. URL: https://cedem.org.ua/news/v-ukrayini-vpershe-zareyestruvaly-avtorski-prava-na-tvory-yaki-mistyat-zobrazhennya-zgenerovani-shi/ (дата звернення 18.12.2024).

31. Газін в. Вестфальська система: випробування XXI століттям 2015. URL: https://zn.ua/ukr/HISTORY/vestfalska-sistema-viprobuvannya-hhi-stolittyam-_.html (дата звернення 16.12.2023).

32. Галянтич М.К., Гармаш О.О. Правове регулювання відносин, пов'язаних із індивідуалізацією фізичної особи, як особистого немайнового права. *Часопис Київського університету права*. 2023. №1. С. 37-43. URL: https://doi.org/10.36695/2219-5521.1.2023.07(дата звернення 16.10.2023).

33. Гапченко О.І. Глобальна цифрова нерівність та її виміри. *Географія та туризм.* 2013. № 24. С. 185-191.

34. Года М. Clearview AI збирає базу фотографій всіх жителів планети: для чого це потрібно компанії. 18.02.2022. URL: https://24tv.ua/tech/clearview-ai-zbiraye-bazu-fotografiy-vsih-zhiteliv-novini-tehnologiy_n1870807 (дата звернення 16.09.2022).

35. Головко О.М. Цифрова культура та інформаційна культура: права людини в епоху цифрових трансформацій. *Інформація і право.* 2019. № 4. С. 37-44.

36. Гололобова Є., Міна А. Цифрові права українців або Декларація цифрових прав людини. 2020. URL: https:// www. businesslaw. org.ua/digital-rights-t/ (дата звернення 16.12.2023).

37. Голубєва Н.Ю. Впровадження інформаційних технологій у судочинство в Україні та світі. Юридичний вісник. 2017. № 2. С.185-194.

38. Голубєва Н.Ю. Деякі пропозиції щодо вдосконалення норм ЦПК, що реалізують електронне судочинство в Україні. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права). 2 т. матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса: Гельветика, 2022. Т. 2. С. 759-762.

39. Голубєва Н.Ю. Електронне судочинство як засіб забезпечення доступності до правосуддя та оптимізації судочинства / Доступ до правосуддя в умовах сталого розвитку: до 30-річчя незалежності України: Колективна монографія / за заг.ред. Ю. Притики та І. Ізарової. Київ: ВД «Дакор», 2021. С. 447-477.

40. Голубєва Н. Ю. Електронне судочинство: міжнародний досвід: монографія [Електронне видання] Одеса: Фенікс, 2020. 204 с. DOI: 10.32837/11300.14039 http://dspace.onua.edu.ua/handle/11300/14039

41. Голубєва Н.Ю. «Електронний суд» за проектом ЦПК України (станом на 10.03.2017 року). Інформаційні технології у судочинстві: матер. всеукр. наук. – практ. конф., яка проводиться в рамках тижня цивільного процесу (Одеса, 18 квітня 2017 р.) /за заг. ред.. д.ю.н., проф.. Голубєвої Н.Ю. Одеса: Фенікс, 2017. С.5-12.

42. Голубєва Н. Ю. Е-адвокат: інформаційні технології в діяльності адвоката. *Адвокатура: минуле, сучасність та майбутнє*: матеріали VII Міжнар. наук-практ. конф. (м. Одеса, 10 листопада, 2017 р.). / за заг. ред. д.ю.н. Н.М. Бакаянової, к.ю.н. Є.С. Хижняка. – Одеса: Гельветика, 2017. С. 285-289.

43. Голубєва Н. Ю. Порядок укладення договорів в електронній формі за законодавством України. Методологічні засади вдосконалення цивільного процесуального права : матеріали Міжнар. наук.-практ. конф. до 150-річчя від дня народження Є. В. Васьковського (8 квітня 2016 р.) / уклад.: І. В. Андронов, Н. В. Волкова, О. В. Сатановська. Одеса: Юрид. л-ра, 2016. С. 3-10.

44. Гончаренко О.А. Право доступу до Інтернету *як* складова прав дитини. *Право та інновації.* 2016. № 4. С. 23-29.

45. Гордієнко Т. Як працює китайський інтернет: без літери N, із забороненим Вінні Пухом та річковими крабами. 10.08.2018. URL: https://ms.detector.media/media-i-vlada/post/21609/2018-08-10-yak-pratsyuie-kytayskyy-internet-bez-litery-n-iz-zaboronenym-vinni-pukhom-ta-richkovymy-krabamy/ (дата звернення 16.07.2023).

46. Горпинюк О. П. Інформаційна приватність та її захист від злочинних посягань в Україні: монографія. Львів: БОНА, 2014. 324 с.

47. Грищук О.В., Слюсарчук Х.Т. Лібералізм та комунітаризм у філософсько-правовому вимірі. Хмельницький, 2018. 301 с.

48. Гуйван П.Д. Недоторканність даних про особисте життя людини як елемент її права на приватність. *Часопис Київського університету права*, 2019. № 4. 179-183. https:// doi.org/10.36695/2219-5521.4.2019__(дата звернення 04.05.2023).

49. Гуйван П.Д. Опосередкування обороту й охорони персональних даних в актах зарубіжного національного законодавства. *Юридичний науковий електронний журнал*. 2020. № 2. С.110-114.

50. Гуйван П.Д. Особливості цивільного захисту інформаційного приватного права особи. *Південноукраїнський правничий часопис.* 2019. № 3. С. 100-104.

51. Давидова І.В., Берназ-Лукавецька О.М. Е-ідентифікація особи в умовах імплементації законодавства європейського союзу. *Південноукраїнський правничий часопис.* 2022. № 4. Ч. 1. С. 213-219.

52. Давидов І.В., Токарева В.О. Захист права на повагу до честі та гідності, ділової репутації, публічних осіб. *Держава та регіони. Серія Право.* 2022. № 1 (75). С. 131-135. URL: http:// www.law. stateandregions.zp. ua/archive/ 1_2022/22.pdf

53. Давидова І.В., Токарева В.О. Цифрова нерівність і право на доступ до Інтернету. *Юридичний вісник***.** 2024. № 6. С. 68-75. URL: http:// yurvisnyk. in.ua/ v6_2024 /10.pdf (дата звернення 16.12.2025).

54. Данилов О.В. США запропонували закон, який передбачає чималі тюремні строки за розповсюдження deepfake порно 19.01.2024. URL: https://mezha.media/2024/01/19/deepfake-porno-law/ (дата звернення 26.12.2024).

55. Дениско Л.М., Пилипенко С.Г., Кулікова І.І. Про перевідкриття гуманізму. *Вісник Харківського національного університету ім. В.Н. Каразіна.* 2014. № 49. С.32- 35.

56. «Ділова репутація», визначення поняття, вплив на ступінь захисту. *Юрист& Закон.* 18.10.2011. № 41 URL: https://jurliga.ligazakon.net/analitycs/ 50497_dlova-reputatsya-viznachennya-ponyattya -vpliv-na-stupn-zakhistu (дата звернення 16.05.2022).

57. Духовна О. Захист репутації в інтернеті. Юридична робота з негативним контентом в YouTube та Google. 17.03.2021. URL: https:// yur-gazeta.com/ dumka-eksperta/zahist-reputaciyi-v- interneti-yuridichna-robota-z-negativnim- kontentom-v-youtube-ta-google.html #:~:text=299%20ЦК%20

України%2C%20 фізична%20 особа, громадських%20чи%20інших%20обов'язків. (дата звернення 16.05.2022).

58. ЄС хоче зробити безпечнішим обмін даними з США. 18 лютого, 2023. URL: https://www.ispc.org.ua/archives/2419 (дата звернення 16.12.2024).

59. ЄСПЛ визнав, що IP-адреса є елементом приватного життя. 10 травня, 2018. URL:

https:// www. legalife.com.ua /2018/06 /10/ iespl-vyznav- shcho-ip- adresa- ie-elementom-pryvatnoho -zhyttia/ (дата звернення 16.07.2023).

60. Життя після смерті. 08.03.2012. URL: https://www.dw.com/uk/в-інтернеті-усі-ми-безсмертні/a-15796399 (дата звернення 16.12.2023).

61. Жуванов Д., Стогній Є. Проблема доменних імен в Україні. *Інтелектуальна власність.* 2003. № 1. С.22-26.

62. Жук Ю.М. Захист від поширення недостовірної інформації в мережі Інтернет. 18.05.2020 URL: https://fidelium.com.ua/zaxist-vid-poshirennya-nedostovirnoi-informaczii-v-merezhi-internet.html (дата звернення 20.10.2022).

63. Жукевич І.В., Застосування штучного інтелекту в механізмі судового контролю за виконанням рішень у цивільному судочинстві України. *Аналітично-порівняльне правознавство.* 2024. № 2. С. 200-203. URL: http://_nbuv.gov.ua/ UJRN/anpopr_2024_2_36 (дата звернення 20.12.2024).

64. Заборона неприйнятних практик використання штучного інтелекту в ЄС. 13.02.2025 URL: https://www.deloitte.com/ua/uk/services/tax/perspectives/tax-and-legal-alert-2025-02-13.html (дата звернення 20.02.2025).

65. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року URL: https:// zakon.rada. gov.ua/laws /show/995_015#Text (дата звернення 20.10.2022).

66. Зміни у визначенні репутації облікового запису Youtube. URL: https://support.google.com/youtube/answer/2797387?hl=uk____(дата звернення 20.12.2023).

67. ІТ-право та інформаційна безпека : навч.-метод. по- сібник / [Є.О. Харитонов, О.І. Харитонова, О.М. Берназ- Лукавецька] Одеса: Фенікс, 2017. 174 с.

68. ІТ-право: Теорія та практика: навч посіб./ авт кол.: за ред. Є.О Харитонова, О.І. Харитонової. Одеса: Фенікс, 2017. 472с.

69. Італійка скоїла самогубство через витік в мережу секс-відео 16 вересня 2016. URL: https:// espreso.tv/ news/2016/09/16/ italiyka_skoyila_ samogubstvo_pislya _oprylyudnennya _v_merezhi_seks_video_z_neyu (дата звернення 20.12.2023).

70. Калітенко О.М. Право на приватність: окремі аспекти. *Шерешевські читання «Проблеми цивільно-правового захисту прав власників у сучасних умовах інтеграційного розвитку України»*: матеріали Всеукр. наук.-практ. (м. Одеса, 7 груд. 2018 р.) / За заг. ред. д.ю.н., проф. Є. О. Харитонова. Одеса: Фенікс, 2018. С. 51-54.

71. Калітенко О.М. Право на забуття: здобуток європейський чи глобальний? Римське приватне право: здобутки європейські та глобальні : матеріали міжнар. колокв. (м. Одеса, 27 жовт. 2018 р.) / За заг. ред. д.ю.н., проф. Є. О. Харитонова. Одеса : Фенікс, 2018. С. 84-86.

72. Калітенко О.М. До питання про державну реєстрацію геномної інформації людини (війна війною, а ми в цифровий світ). Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття»: матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) Одеса: Гельветика, 2022. Т. 2. С. 607-612.

73. Карандась М.В. Цифрові права у цивільному законодавстві України. *Науковий вісник Ужгородського національного університету.* Науковиґ вісник Ужгородського Національного Університету, 2023. №75 (1) С. 173-180. URL: http://nbuv. gov.ua/UJRN/nvuzhpr_2023_75(1)__30 (дата звернення 20.12.2024).

74. Кармаза О., Грабовська О. Електронна особа (особистість) як суб'єкт правовідносин у цивілістичному процесі. *Підприємництво, господарство і право.* 2021. № 2. С. 5-10.

75. Кобижча Н. «Цифрова смерть та безсмертя» у сучасному науковому дискурсі. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2023. № 6(1). С. 205-216. URL: https://doi.org/10.31866/2617-796X.6.1.2023.283991

76. Кодекс суддівської етики затверджене рішенням XX чергового з'їзду суддів України від 18.09.2024. URL: https://zakon .rada.gov.ua /rada/show/n000 1415-24#Text (дата звернення 20.11.2024).

77. Конвенція про захист прав людини і основоположних свобод 04.11.1950. Рим. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text_(дата звернення 21.10.2022).

78. Конституція України: Верховна Рада України від 28.06.1996. Відомості Верховної Ради України. 1996. № 30. ст. 141. URL: https:// zakon.rada.gov.ua /laws/show/254к /96-вр#Text (дата звернення 20.07.2022).

79. Концепція розвитку штучного інтелекту в Україні схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення 20.11.2024).

80. Концепція розвитку системи електронних послуг в Україні схвалену розпорядженням Кабінету Міністрів України від 16 листопада 2016 р. № 918-р. Офіційний вісник України. 2016. № 99. ст. 259. URL: https://zakon.rada.gov.ua/laws/card/918-2016-р (дата звернення 20.07.2022).

81. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки, схвалена Розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р. Офіційний вісник України. 2018. № 16. ст. 70. URL: https:// zakon. rada.gov. ua/laws/show/67-2018-р#Text (дата звернення 20.07.2022).

82. Концепції оновлення Цивільного Кодексу України. Київ: Видавничий дім АртЕк, 2020. 128 с.

83. Колдомасов А. Цензура китайського інтернету: як це працює? 2019. URL: https://adastra.org.ua/blog/cenzura-kitajskogo-internetu-yak-ce-pracyuye_(дата звернення 23.04.2022).

84. Костенко О.В. Електронна юрисдикція, метавсесвіт, штучний Інтелект, цифрова особистість, цифровий аватар, нейронні мережі: теорія, практика, перспективи. *Наукові інновації та передові технології.* 2022. № 2(4). С. 54-78. URL: http://perspectives.pp.ua/index.php/nauka/article/view/1038/1037 (дата звернення 20.12.2023).

85. Користувацька угода Facebook URL: https://www.facebook.com/terms.php (дата звернення 20.01.2025).

86. Кодекс законів про працю України № 322-VIII від 10.12.71. Відомості Верховної Ради УРСР 17.12.1971. URL: https://zakon.rada.gov.ua/laws/show/322-08/print (дата звернення 20.12.2023).

87. Кравченко А. Цифрова ідентичність людини. Як її захистити? 09.2021. URL: https://www.ukrinform.ua/rubric-society/3316842-cifrova-identicnist-ludini-ak-ii-zahistiti.html (дата звернення 20.03.2023).

88. Кудіна М. «Верховний суд» Facebook: чи принесе він прав... – Інтернет Свобода. 2021. URL: https://netfreedom.org.ua/article/verhovnij-sud-facebook-chi-prinese-vin-pravosuddya-u-socmerezhu(дата звернення 20.09.2022).

89. Кудінська І., Сандул Г. Чи має працівник право бути офлайн у позаробочий час? 29.04.2021 URL: https://hrliga.com/index.php?module=news&op=view&id=22973 (дата звернення 08.12.2022).

90. Кулініч О.О. Загальні положення про інформацію з обмеженим доступом в цивільному праві: монографія. Одеса: Букаєв Вадим Вікторович, 2008. 243 с.

91. Кулініч О.О. Доменне ім’я як похідний засіб індивідуалізації інформаційних ресурсів фізичних та юридичних осіб у мережі Інтернет. *Актуальні проблеми держави і права*. 2009. С. 195-201.

92. Кулініч О.О. Доменне ім’я як засіб індивідуалізації інформаційних ресурсів фізичних та юридичних осіб в мережі Інтернет. *Актуальні проблеми політики*. 2009. № 38. С. 159-165.

93. Клименко А.А., Каландей В.О. Проблеми реалізації права інтелектуальної власності на інформаційні ресурси в Україні. *Актуальні проблеми приватного права*: матер. Всеукр. наук.-практ. інтернет-конф. (Ірпінь, 28 листопада 2019 р.). Ірпінь: Університет державної фіскальної служби України, 2019. С. 93-96.

94. Коршакова О.М. Окремі аспекти правового регулювання доменних імен в україні. Право і суспільство. 2017. № 3(2). С. 52-55.

95. Лаптєва Т. О. Методи виявлення та припинення розповсюдження недостовірної інформації в Інтернеті. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання:* матеріали Всеукр. наук.-практ. конф., м. Київ, 2 грудня 2021 р. – Київ-Одеса: Фенікс, 2021. С. 290-293.

96. Лебедєва Г.В. Захист прав та інтересів осіб, порушених внаслідок використання об'єктів права інтелектуальної власності. Дисертація на здобуття ступеня доктора філософії. Одеса. 2021. 207 с.

97. Лесько Н., Антонов М. Цифрові права людини в епоху глобалізації. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*. 2021. №. 3 (31). С. 160-166. URL: http://nbuv.gov.ua /UJRN/ vnulpurn_ 2021_8_3_24(дата звернення 08.12.2023).

98. Майданик Н. Право на доменне ім'я в мережі інтернет: поняття і правова природа. ресурс. *Юридична наука.* 2009. № 6. С. 81-86.

99. Майданик Р.А. Смарт-контракт криптоактивів у цивільному праві України. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. 2024. № 127(1). С. 39-44. https: //doi.org /10.17721/1728-2195/2024/1.127-7 (дата звернення 20.12.2024).

100. Мамедов Г.А. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? 8 червня 2022. URL: https://nv.ua/_ukr/opinion/ viyna-v-ukrajini-yak- cifrova-kriminalistika- vikrivaye-zlochini-rf-v-ukrajini- novini-ukrajini-50248411.html (дата звернення 20.10.2023).

101. Марчук М. І. Право на інтернет як базове право людини. *Протидія кіберзагрозам та торгівлі людьми:* зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 26 листоп. 2019 р.) Харків: ХНУВС, 2019. С. 116-119.

102. Марценко Н.С. Використання штучного інтелекту у цивільному судочинстві. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання:* матеріали Всеукр. на- ук.-практ. конф., м. Київ, 2 грудня 2021 р. Київ- Одеса: Фенікс, 2021. С. 59-65.

103. Марценко Н.С. Права людини та сучасні технології штучного інтелекту. *Права людини – пріоритет сучасної держави:* збірник матер. Всеукр. наук.-практ. Інтернет-конференції (10 грудня 2020 року, м. Одеса) / відп. ред. М. Р. Аракелян. Одеса : Гельветика, 2020. С. 223-226.

104. Мацик В. Перспективи розвитку превентивної медицини. *Актуальні проблеми менеджменту та публічного управління в умовах інноваційного розвитку економіки.* Всеукраїнська-наукова практична конференція з міжнародною участю: 15 травня 2020. Тернопіль: ТНЕУ.2020. С. 116-119.

105. Міжнародний пакт про громадянські і політичні права. Генеральна Асамблеєя ООН. 16 грудня 1966 року. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення 18.10.2023).

106. Міхровська М.С. Діджитизація, діджиталізація, цифрова трансформація: зміст та особливості. International scientific journal «Grail of Science». № 1 (February), 2021. URL: https://www.researchgate.net/publication/349715623_ DIDZITIZACIA DIDZITA LIZ ACIA _C IFROVA _TRANSFORMACIA _ZMIST_TA_OSOBLIVOSTI (дата звернення 08.12.2023).

107. Мічурін Є.О. Ідентифікація і індивідуалізація фізичної особи у компьютерній мережі Інтернет: правові аспекти. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО».* 2022. 34. С. 91-96.

108. Мічурін Є.О. Правова природа штучного інтелекту. *Форум права*. 2020. № 5. С. 67-75.

109. Можливості й небезпеки чіпування: чому компанія Ілона Маска прагне вживляти технології в людський мозок 21.05.2023. URL: https://weukraine.tv /top/mozhlyvosti-j-nebezpeky- chipuvannya-chomu-kompaniya-ilona-maska -pragne-vzhyvlyaty -tehnologiyi-v-lyudskyj -mozok/# goog_ rewarded (дата звернення 08.12.2023).

110. Мукомела І.В. Право на доступ до Інтернету: проблеми визначення та забезпечення. *Вісник Національної академії правових наук України.* Харків, 2016. № 4 С. 77-85. URL: http:// visnyk.kh.ua /web/uploads /pdf/ilovepdf _com-77-85.pdf (дата звернення 08.12.2023).

111. Мяловицька Н.А. Автономія: поняття, принципи, класифікація. Альманах права. 2012. № 3. С. 93-97.

112. Накладення КЕП. URL:https://se.diia.gov.ua/faq/9 (дата звернення 08.12.2023).

113. Небезпечна гавань. Американські стандарти визнанні недостатніми для захисту персональних даних. *Закон і бізнес.* №41 (1235). URL: https:// zib.com.ua/ ua/print/119128- amerikanski_standarti _viznani_nedostatnimi_dlya_zahistu_pers.html (дата звернення 08.12.2023).

114. Некіт К. Г. Доменне ім’я як об’єкт цивільних прав. *Часопис цивілістики.* 2017. № 23. С. 40-44.

115. Некіт К.Г. Користувацька угода (terms of service) як підстава виникнення права власності на віртуальне майно. *Право та інновації.* 2020. № 4 (32). С.62-67.

116. Некіт К. Г. Персональні дані та індустріальні дані як об’єкти права власності: оцінка перспектив. *Часопис цивілістики*. 2020. № 36. С. 57-64.

117. Некіт К. Г. Поняття та правова природа акаунта в соціальній мережі. *Часопис цивілістики.* 2018. № 30. С. 60-65.

118. Новий тренд Instagram – віртуальні моделі: хто це такі і як це працює. 18 серпня 2019. URL: https://ukr.media/fashion/399308/ (дата звернення 08.12.2023).

119. Огнев'юк Т., Штучний інтелект і верховенство права: світова практика та можливості для України. Слово національної школи суддів України. 2023. № 4 (45) С. 65-70. DOI 10.37566/2707-6849-2023-4(45)-5

120. Окрема думка від 08.02.2024 № 925/200/22 Верховний Суд. Касаційний господарський суд URL: https://verdictum.ligazakon.net/document/117074064 (дата звернення 08.11.2024).

121. Окремі питання спадкування: Роз'яснення Міністерства Юстиції України від 11.10.2011. URL: https://zakon.rada.gov.ua/laws/show/n0064323-11(дата звернення 08.05.2023).

122. Омельчук О.В., Левицька Л.М. Діджиталізація суспільства і ґаджет-залежність сучасної молоді – покоління Digital Natives. *Науковий часопис НПУ імені М.П. Драгоманова*. 2020. № 3. С. 296-300. URL: https://enpuir.npu.edu.ua/handle/123456789/32896

123. Основи ІТ-права:навч.посіб./ Т.В. Бачинський, Р.І. Радейко, О.І. Харитонова і інші. К.: Юрінком Інтер, 2017. 208 с.

124. ООН визнала доступ до Інтернету невід'ємним правом людини 07.06.2011. URL: https://www.unian.ua/science/504107-oon-viznala-dostup-do-internetu-nevidemnim-pravom-lyudini.html (дата звернення 08.05.2023).

125. Панченко Т.В. Автономія. Велика українська енциклопедія. URL: https:// vue.gov.ua/Автономія (дата звернення 20.04.2023).

126. Парламент прийняв Закон про державну реєстрацію геному людини**.** 10.07.2022. URL: https://yaizakon.com.ua/parlament-prijnyav-zakon-pro-derzhavnu-reyestratsiyu-genomu-lyudini/ (дата звернення 08.11.2022).

127. Петровська А.О. Цифрова трансформація у сфері судочинства. Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання: матеріали Всеукр. на-ук.-практ. конф., м. Київ, 2 грудня 2021 р. Київ Одеса: Фенікс, 2021. С. 65-69.

128. *Петрів М.В. Доменні* імена є *засобами* адресації в цифровому середовищі. *Часопис цивілістики.* 2019. № 33. С. 92-96.

129. Писаренко Н.Б. Верховенство права в адміністративному судочинстві: від доктринальної ідеї до практичної імплементації. *Вісник Національної академії правових наук України*. 2018. № 1. Т. 25. С.134-145.

130. Плескач В.Л., Рогушина Ю.В. Агентні технології: Монографія. Київ. 2005. 344 с.

131. Політика конфіденційності. Instagram. URL: https://privacycenter.instagram.com/policy/

132. Пода Р.В., Керноз Н.Є. Штучний інтелект в рішеннях суду України. Матеріали Міжнародної науково-методичної конференції «Модернізація вищої освіти та забезпечення якості освітньої діяльності в умовах європейської інтеграції» 18 жовтня 2024 р. С. 436-438. URL: https:// repo.btu. kharkov.ua/ bitstream/ 123456789/58999/ 1/conf-18-10-24-materialy-161.pdf (дата звернення 08.12.2024).

133. Податковий кодекс України 2.12.2010 № 2755-VI. Відомості Верховної Ради України. 2011. № 13-14. ст.112. URL: https:// zakon. rada.gov.ua /laws/show/2755-17#Text (дата звернення 12.08.2022).

134. Порядок ведення Єдиного державного демографічного реєстру та надання з нього інформації, взаємодії між уповноваженими суб'єктами, а також здійснення ідентифікації та верифікації затверджений постановою Кабінету Міністрів України від 18.10.2017 № 784. Офіційний вісник України. 2017. № 86. ст. 38. URL: https://zakon.rada.gov.ua/laws/show/784-2017-п#Text (дата звернення 08.08.2022).

135. Постанова від 19.09.2018 № 806/3265/17 Верховний Суд України. URL: https://verdictum.ligazakon.net/document/76822787 (дата звернення 08.05.2023).

136. Правова природа особистих немайнових прав особи та прав на віртуальні активи в умовах цифровізації: монографія/ за редакцією Булеци С. Б., Менджул М. В. Ужгород: РІК-У, 2023. 272с.

137. Права людини онлайн: Порядок денний для України / В. Володовська, М. Дворовий. Київ: Лабораторія цифрової безпеки, 2019. 56 с. URL:

https://dslua.org/ wp-content/uploads/2019/ 12/DRA_FINAL_ UKR.pdf (дата звернення 08.07.2022).

138. Права людини та верховенство закону у інформаційному суспільстві. Декларація Комітету міністрів з прав людини та верховенства права у інформаційному суспільстві CM(2005)56 13 мая 2005 URL: https:// rm.coe.in t/16802e3e96 (дата звернення 08.05.2022).

139. Право на приватність Резолюція ПАРЄ № 1165. 1998. URL: https:// cedem.org.ua/library/ rezolyutsiya-1165-1998-pravo -na-pryvatnist/ (дата звернення 08.05.2022).

140. Проєкт Закону України: Про захист персональних даних від 25.10.2022 № 8153 URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (дата звернення 08.05.2024).

141. Проєкт Закону України: Про єдину систему відеомоніторингу стану публічної безпеки від 20.02.2024 № 11031. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733 (дата звернення 08.09.2024).

142. Проєкт Закону України: Про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до Інтернету). від 16.04.2014 № 4715. URL: http://w1.c1.rada.gov.ua/pls/zweb2/ webproc4_1?pf3511=50669. (дата звернення 08.08.2022).

143. Проєкт Закону України: Про внесення змін до Цивільного кодексу України щодо унормування питання прийняття спадщини спадкодавець якої перебуває за кордоном від 09.10.2023 № 10134. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/42910 (дата звернення 08.11.2023).

144. Про авторське право і суміжні права. Закон України від 1.12.2022 № 2811-IX. *Відомості Верховної Ради.* 2023. № 57. ст.166. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (дата звернення 08.05.2023).

145. Про банки та банківські діяльність: Закон України від 7.12.2000 № 2121-III URL: https:// zakon.rada.gov.ua/laws/show/2121-14#Text (дата звернення 08.08.2023).

146. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX. *Відомості Верховної Ради України.* 2022. № 15. ст. 47. URL: https://zakon.rada.gov.ua/laws/show/2074-IX#Text. (дата звернення 08.08.2023).

147. Про внесення змін до деяких законодавчих актів України щодо удосконалення правового регулювання дистанційної, надомної роботи та роботи із застосуванням гнучкого режиму робочого часу: Закон України від 04.02.2021 № № 1213-IX. *Відомості Верховної Ради України.* 2021. № 20. ст.178. URL: https:// zakon.rada. gov.ua/laws/show/ 1213-20#n37 (дата звернення 07.09.2023).

148. Про державну реєстрацію геномної інформації людини. Закон України від 09.07.2022 № 4265. *Офіційний вісник України.* 2022. № 88. ст. 9. URL: https:// zakon.rada.gov.ua/ laws/show/2391-20#Text (дата звернення 07.09.2023).

149. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень: Закон України від 01.07.2004 № 1952-IV. Відомості Верховної Ради України. 2004. № 51. ст. 553. URL: http://zakon5.rada.gov.ua/laws/ show/1952-15. (дата звернення 20.08.2022).

150. Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань: Закон України від 15.05.2003 № 755-IV. Відомості Верховної Ради України. 2003. № 31-32. ст.263. URL: http:// zakon2.rada.gov.ua/laws/show/755-15. (дата звернення 11.08.2022).

151. Про електрону ідентифікацію та довірчі послуги для електронних транзакцій, в межах внутрішнього ринку Регламент Європейського Парламенту та Ради ЄС № 910/2014 від 23.07.2014 URL: https://zakon. rada.gov.ua /laws/show/984_016-14#Text (дата звернення 11.08.2022).

152. Про електронну ідентифікацію та електронні довірчі послуги: Закон України 5.11.2017 № 2155-VIII. Відомості Верховної Ради. 2017. № 45. ст.400. *Відомості Верховної Ради.* 2017. № 45. ст.400. URL: https://zakon. rada.gov.ua/laws/show/2155-19. (дата звернення 11.08.2022).

153. Про електронні комунікації: Закон України від 16.12. 2020 № 1089-IX. *Офіційний вісник України.* 2021. № 6. С. 10. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення 11.08.2022).

154. Про електронну комерцію: Закон України від 3.09.2015 № 675-VIII. *Відомості Верховної Ради.* 2015. № 45. ст.410. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення 08.12.2022).

155. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус. Закон України 20.112012 № 5492-VI. *Відомості Верховної Ради.* 2013. № 51. ст.716. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text (дата звернення 08.08.2022).

156. Про запобігання та протидію легалізації (відмиванню) доходів, одержанних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знащення: Закон України від 6.12.2019 № 361-IX. *Відомості Верховної Ради України.* 2020. № 25. ст.171. URL: https:// zakon. rada.gov.ua/laws/ show/361-20#Text (дата звернення 08.08.2022).

157. Про захист прав і гідності людини щодо застосування біології та медицини: Конвенція про права людини та біомедицину. Рада Європи. Ов'єдо. 4.04.1997. URL: https://zakon.rada.gov.ua/laws/show/994_334#Text (дата звернення 05.09.2022).

158. Про захист честі, гідності та ділової репутації. Постанова Верховного Суду України від 18.05.2020 у справі №522/18103/14 URL: https:// reyestr. court. gov.ua/ Review/89928850 (дата звернення 08.08.2022).

159. Про інформацію: Закон України 2.10.1992 № 2657-XII URL: https: //zakon.rada. gov.ua/laws/show/2657-12#Text (дата звернення 05.09.2022).

160. Про Національну стратегію у сфері прав людини: Указ Президента України №119/2021 від 24 березня 2021 року URL: https:// www. president.gov.ua/ documents/ 1192021-37537 (дата звернення 08.08.2022).

161. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 9 січня 2007 № 537-V. *Відомості Верховної Ради України.* 2007. № 12. ст.102. URL: https://zakon. rada.gov. ua/laws/ show/ 537-16#Text (дата звернення 08.08.2022).

162. Про організацію формування та обігу кредитних історій. Закон України від 23.06.2005 № 2704-IV. *Відомості Верховної Ради України.* 2005. № 32. ст.421. URL: https:// zakon.rada. gov.ua/laws/show/2704-15#Text (дата звернення 12.08.2022).

163. Про погодження проєкту розпорядження Кабінету Міністрів України «Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні» із зауваженнями: Вища рада правосуддя лист від 9.02.2021 № 283/0/15-21 URL: https://hcj.gov.ua/sites/default/files/field/file/283_09.02.2021.docx (дата звернення 15.08.2022).

164. Про ратифікацію Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства: Закон України від 20.06.2012 № 4988-VI. *Відомості Верховної Ради.* 2013. № 19-20. ст.180. URL: https:// zakon.rada.gov. ua/laws/ show/4988 -17#Text (дата звернення 27.07.2022).

165. Про систему електронних підписів, що застосовується в межах Співтовариства. Директива 1999/93/ЄС Європейського Парламенту та Ради від 13.12.1999. URL: https:// zakon.rada.gov.ua/ laws/show/994_240 #Text (дата звернення 20.08.2022).

166. Про страхування Закон України: від 18.11.2021 № 1909-IX. URL: https://zakon.rada.gov.ua/laws/show/1909-20#Text (дата звернення 22.07.2022).

167. Про судову практику в справах про захист гідності та честі фізичної особини, а також ділової репутації фізичної та юридичної особини: Постанова Пленуму Верховного Суду України від 27.02.2009 №1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09#Text (дата звернення 22.07.2022).

168. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних: Управління Верховного комісара ООН. Центр прав людини. Юридична школа Каліфорнійського университету Берклі. 2020 р. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення 22.07.2023).

169. Прохоров П.А. Порядок ухвалення судових рішень у цивільному процесі України. Дисертація на здобуття ступеня доктора філософії. Національний університет «Одеська юридична академія». Одеса. 2021. 233с.

170. Пункт незламності URL: https://nezlamnist. gov.ua (дата звернення 22.07.2022).

171. Податковий Кодекс України: Верховна Рада України від 2.12.2010 р. № 2755-VI Відомості Верховної Ради України. 2011. № 13-14. ст.112. URL: https://zakon.rada.gov.ua/laws/show/2755-17/print (дата звернення 22.07.2022).

172. Пономаренко К.І. Інформаційна приватність як об'єкт правового регулювання. *Право і суспільство.* 2011. № 5. С. 113-118.

173. Радутний О.Е. Великі дані: кореляції та причинність (кримінально-правовий аспект). *Інформація і право.* 2023. №2 (45). С. 94-112.

174. Размєтаєва Ю.С. Цифрові права людини та проблеми екстериторіальності в їх захисті. *Право та державне управління.* 2020. № 4. С. 18-23.

175. Размєтаєва Ю.С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання. *Науковий вісник Ужгородського національного університету*. *Серія: Право.* 2016. № 37(1). С. 43-46.

176. Рішення Конституційного Суду Цкраїни у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12/print (дата звернення 22.07.2022).

177. Рішення Суворовського районного суду м. Одеси у справі від 19 вересня 2024 № 523/21237/23 URL: https://reyestr.court.gov.ua/Review/121759081 (дата звернення 10.03.2025).

178. Рішення Святошинського районного суду м. Києва у справі від 20 лютого 2025 № 759/6452/24 URL: https://reyestr.court.gov.ua/Review/125300649 (дата звернення 10.03.2025).

179. Рішення Корабельного районного суду м. Миколаєва у справі від 19 лютого 2025 № 488/4536/24. URL: https://reyestr.court.gov.ua/Review/125263293 (дата звернення 10.03.2025).

180. Рішення Жовтневого районного суд міста Кривий Ріг у справі від 17 лютого 2025 № 212/6925/24. URL: https://reyestr.court.gov.ua/Review/125217719 (дата звернення 12.03.2025).

181. Рішення Новоодеського районного суду Миколаївської області у справі від 12 лютого 2025 № 482/2102/24. URL: https://reyestr.court.gov.ua/Review/125134531 (дата звернення 10.03.2025).

182. Рішення Бердичівського міськрайонного суду Житомирської області у справі від 28 січня 2025 № 274/8488/24. URL: https://reyestr.court.gov.ua/Review/125163619(дата звернення 10.03.2025).

183. Рішення Валківського районного суд Харківської області у справі від 15 січня 2025 № 615/2049/24. URL: https:// reyestr.court. gov.ua /Review/ 124519593 (дата звернення 10.03.2025).

184. *Розгон* О.В. *Передання прав за ліцензійним договором на використання програмного забезпечення* або *комп'ютерних програм*. *Юридичний науковий електронний журнал.* 2021. № 9. С. 86-90.

185. Романов Р. В. пошуках досконалої моделі правового регулювання доступу до інформації. *Свобода висловлювань і приватність.* 2000. № 4. С. 6.

186. Роман Р. Фільтрація і блокування контенту в мережі Інтернет: досвід Китайської Народної Республіки. 06.06.2017. URL: https://ilaw. center/ filtratsiya-i- blokuvannya -kontentu- v-merezhi-internet-dosvid- kytajskoji-narodnoji-respubliky/ (дата звернення 25.07.2022).

187. Ромовська З. В. Українське сімейне право: Академічний курс / З. В. Ромовська. – Київ: Правова єдність, 2009. 500 с.

188. Самодурова Д. А. Інтелектуальні агенти та мультиагентні системи у виробництв. *Економічний вісник Донбасу*. 2019. № 2(56). С. 179-186.

189. Сафончик О.І. Актуальні питання цивільно-правового захисту та охорони персональних даних в мережі інтернет за законодавством України.

Юридичний вісник. №5. 2023. С. 93-99. URL: http://yurvisnyk.in.ua/v5_2023/12.pdf (дата звернення 25.07.2024).

190. Сексуальна експлуатація дорослих. Meta. URL: https:// transparency. fb.com/ru-ru/policies/ community-standards/ sexual -exploitation- adults/? source=https%3A %2F%2Fwww.facebook.com %2Fcommunitystandards %2Fsexual_exploitation_adults(дата звернення 25.04.2023).

191. Система ID.GOV.UA – найкращий сервіс онлайн-ідентифікації в Україні. URL: https://www.kmu.gov.ua/news/sistema-idgovua-najkrashchij-servis-onlajn-identifikaciyi-v-ukrayini (дата звернення 25.12.2022).

192. Січевлюк В.А. Динаміка індивідуальної правосуб'єктності як предмет пізнання загальної теорії права. *Науковий вісник Ужгородського національного університету*. 2018. № 51. С. 41-48.

193. Світлак І. І. Трансформація цивільних правовідносин з надання послуг в умовах цифровізації: теоретичні та практичні аспекти : автореф. дис.... д-ра юрид. наук: 12.00.03. Тернопіль, 2021. 36 с.

194. Серьогін В. Зміст і обсяг права на недоторканність приватного життя (прайвесі). *Вісник Академії правових наук України.* 2010. № 4. С. 88-97.

195. Скляренко І.В. Сучасні перспективи заміни суддів у цивільному судочинстві на технологію штучного інтелекту. *Юридичний науковий електронний журнал*. 2024. № 4. С. 153-156.

196. Сканування за ходою і формою тіла: у Китаї запускають систему тотального стеження. 11 листопада 2018. URL: https://konkurent.ua/publication/32528/skanuvannya-za-hodou-i-formou-tila-u-kitai-zapuskaut-sistemu-totalnogo-stezhennya

197. *Софіюк Т.О. Прайвесі* і *концепція поколінь прав людини. Часопис Київського університету права*. 2020. № 2. С. 255-258.

198. Сокуренко В.А., Хрякова Н.О. Право на приватність у мережі інтернет у контексті європейської системи захисту прав людини. *Юридичний науковий електронний журнал.* 2021. № 4. С. 280-284.

199. Спадкування акаунту в Facebook: що відбувається зі сторінкою людини, яка померла? May 16, 2023. URL: https://cedem.org.ua/consultations/spadkuvannya-akauntu-facebook/ (дата звернення 25.10.2023).

200. Спадкування віртуальних активів. К*омпанія Dynasty Law & Investment. 24.01.2024.* URL: https://eba.com.ua/spadkuvannya-virtualnyh-aktyviv/(дата звернення 25.04.2024).

201. Стандарти і вимоги щодо послуг і вражень Airbnb. URL: https://www.airbnb.com.ua/help/article/1451 (дата звернення 25.10.2023).

202. Стефанчук М.О. Теоретичні засади правосуб'єктності фізичних осіб та особливості її здійснення. Дисертація та здобуття доктора юридичних наук. Київ. 2020. 473с.

203. Стефанчук Р.О. Система особистих немайнових прав фізичних осіб у сфері сімейних відносин: до питання вдосконалення. *Університетські наукові записки.* 2006. № 2 (18). С. 107-111.

204. Стефанчук Р.О. Особисті немайнові права фізичних осіб (поняття, зміст, система, особливості здійснення та захисту): монографія. К.: КНТ, 2008. 626 с.

205. Стратегія розвитку Верховного Суду на 2023 – 2027 роки (проєкт станом на травень 2023) URL: https:// drive.google.com /file/d/1pFBJy BafrCCoopn HEOS5WFF q0ANSBk-t/view (дата звернення 25.10.2023).

206. Стрельцов Є. Л. Державний суверенітет і суверенітет особистості: проблеми взаємовідносин. Правове забезпечення ефективного виконання рішень і застосування практики Європейського суду з прав людини : матер. 2-ї Міжнар. наук. - практ. конф. (Одеса, 20-21 вересня 2013 р.) / за ред. С. В. Ківалова; НУ «ОЮА». Одеса: Фенікс, 2013. С. 48-60.

207. Супрун Г.Г. Ідентичність індивіда в цифрову епоху соціальних комунікацій. *Філософські обрії.* 2020. № 43. С. 85-94.

208. Тарасенко Л.Л. Право на доступ до Інтернету. Інтелектуальна власність, інформаційне та корпоративне право. *Вісник Львівського університету.* 2020. № 71. С. 53-61.

209. Тарасенко Л. Доменне ім`я як засіб індивідуалізації в цифровому середовищі URL: http://tspartners.lviv.ua/articles/domenne-imja-jak-zasib-indyvidualizatsiji-v-tsyfrovomu-seredovyschi/

210. Тищук Н. О. Вчинення малолітніми та неповнолітніми особами правочинів в мережі Інтернет. Дисертація на здобуття ступеня доктора філософії. Національний університет «Одеська юридична академія», Одеса, 2021. 237 с.

211. Токарева В.О. Авторське право у цифрову добу. *Часопис цивілістики.* 2017. №26. С. 93-98.

212. Токарева В.О. Анонімність в мережі Інтернет. *Law in the postmodern epoch: general characteristics and manifestation particularities in separate law branches:* Scientific monograph. Riga, Latvia: Baltija Publishing, 2023. С. 601-617.

213. Токарева В.О. Віртуальна ідентичність як проекція фізичної особи у мережі Інтернет. *The European dimension of modern legal science:* Scientific monograph. Riga, Latvia: Baltija Publishing, 2022. С. 406-418.

214. Токарева В.О. Деякі питання щодо категорії «віртуальна ідентичність» у мережі Інтернет. *Розвиток громадянського суспільства як необхідна складова європейської інтеграції України:* матеріали Всеукраїнської науково -практичної конференції (м. Київ, 06 жовтня 2022 р.). Львів-Торунь: Liha-Pres, 2022. С. 292-295.

215. Токарева В. О. До питання виникнення правосуб'єктності фізичної особи у мережі Інтернет. *І Міжнародна науково-практична конференція Таврійського національного університету до 160-ї річниці від дня народження В. І. Вернадського:* матеріали Міжнародної науково-практичної конференції, 16–17 березня 2023 р., м. Київ. Ч.1. Львів-Торунь: Liha-Pres, 2023. С. 57-61.

216. Токарева В.О. До питання прийняття рішень із застосування алгоритмів**.** *Публічне та приватне право.* 2023. № 1. С. 30-35.

217. Токарева В.О. До питання права на зображення (голограму) фізичної особи після смерті в умовах поширення технологій ШІ. *Часопис цивілістики.* 2024. № 54. С. 43-48.

218. Токарева В. О. Дотримання GDPR в умовах COVID-19. *Інформаційні технології в умовах оновлення цивільного законодавства:* матер. Всеукр. кругл. столу (м. Одеса, 13 черв. 2020 р. / За заг. ред. О. І. Харитонової, Є. О. Харитонова. Одеса: Фенікс, 2020. С. 60-62.

219. Токарева В.О. Інтелектуальна власність КНР: на шляху інновацій. *Науковий Вісник МГУ.* 2018. № 32. С. 53-56.

220. Токарева В.О. Наслідки порушення прав інтелектуальної власності китайськими товаровиробниками. *Часопис цивілістики.* 2016. № 20. С. 202-206.

221. Токарева В.О. Обчислювальна творчість (щодо питання творчості штучного інтелекту). *Часопис цивілістики*. 2018. № 30. С. 38-43.

222. Токарева В.О. Онлайн платформи: виклик авторському праву у цифрову добу. *Часопис цивілістики.* 2018. № 29. С. 107-111.

223. Токарева В.О. Окремі питання легалізації сирітських творів. *Recht der Osteuropäischen Staaten.* 2019. №1. С. 197-201.

224. Токарева В.О. Окремі аспекти сирітских творів в умовах інтеграційних процесів. *Jurnaluljuridic.* 2019. №3. С. 97-101. http://www.jurnaluljuridic.in.ua/archive/2019/3/part_1/22.pdf

225. Токарева В.О. Окремі питання реалізації права на видалення. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 2. С. 42-47.

226. Токарева В.О. Обчислювальна (Алгоритмічна) творчість: постановка проблеми. *Visegrad Jurnal on Human Rights.* 2019. № 2. С. 150-155.

227. Токарева В.О. Окремі питання управління майном фізичної особи**.** *Юридичний науковий електронний журнал.* 2024. № 4. С.129-131.

228. Токарева В.О. Похідні твори у галузі сучасного мистецтва. *Науковий вісник публічного та приватного права.* 2019. № 6. С. 35-40.

229. Токарева В.О. Проблемні питання творчості в умовах цифрової доби. *European political and law discourse*. 2019. №2. С.123-128.

230. Токарева В.О. Порушення прав на торговельні марки в мережі Інтернет. *Юридичний науковий електронний журнал.* 2023. №10. С.141-144.

231. Токарева В.О. Проблемні аспекти творчості в епоху цифрових трансформацій. Взаємодія громадянського суспільства, особи і держави: вектор удосконалення: *Міжнародна науково-практична конференція:* (м. Київ, 22 червня 2021) Київський регіональний центр НАПрН, 2021. С. 179-182.

232. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики.* 2023. № 49. С. 32-37.

233. Токарева В.О. Правове регулювання застосування систем віддаленої біометричної ідентифікації в ЄС. *Публічне та приватне право.* 2023. № 2. С. 3-8.

234. Токарева В. Реалізація сімейної правоздатності фізичної особи за допомогою мережі Інтернет. *Юридичний бюлетень.* 2023. № 29. С. 134-141.

235. Токарева В.О. Розвиток цифрової ідентичності як елементу сервісної держави в умовах війни. *Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: монографія*. За ред.: Є. О. Харитонова, О. І. Харитонової, К.Г. Некіт; НУ «Одеська юридична академія». Одеса: Фенікс, 2023. С.86-97.

236. Токарева В.О. Сумлінне використання та похідні твори у сучасному мистецтві. *Таврійський національний університет імені В.І. Вернадського.* 2020. № 31 (70). № 2. С. 121-125.

237. Токарева В.О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. Актуальні проблеми вітчизняної юриспруденції. 2022. № 3. С. 47-52. URL: http://apnl._dnu.in.ua/ 3_2022/8. pdf

238. Токарева В.О. Умови охороноздатності об’єктів авторського права. *Приватне та публічне право.* 2019. № 3. 39-43.

239. Токарева В.О. Формування категорії «віртуальна ідентичність» у мережі Інтернет. *Часопис Цивілістики*. 2022. № 45. С. 63-67.

240. Токарева В.О. Щодо визначення персональних даних в умовах Євроінтеграційних процесів. *Південноукраїнський правничий часопис.* 2022. № 4. Том 3. С. 169-174.

241. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Публічне та приватне право.* 2022. № 4. С. 35-40.

242. Токарева В.О. Щодо питання інформаційної природи авторського права. *Часопис цивілістики.* 2019. № 33. С. 61-66.

243. Токарева В.О. Щодо питання творчості та штучного інтелекту. *Прикарпатський юридичний вісник.* 2018. № 1(22). С. 55-58.

244. Токарева В.О. Щодо питання захисту прав інтелектуальної власності. *Часопис Цивілістики.* 2020. №. 36. 51-56.

245. Токарева В.О., Личко В.С. Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал*. 2024. №4. С. 848 -851.

246. Токарева В.О., Личко В.С. Спадкування об’єктів в мережі Інтернет: досвід західних держав. *Часопис цивілістики.* 2024. № 53. С.41-46.

247. ТОП-10 українських дітей-відеоблогерів, чиї канали мають багато підписників на YouTube, заробляють мільйони. URL: https://_www. ukrinform.ua /rubric-culture/27493 66-top10- najbagatsih-ditejvideoblogeriv-ukraini.html (дата звернення 25.10.2023).

248. Удовенко Ж.В., Басиста І.В. Використання штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. *Штучний інтелект у правовій практиці: межі та можливості*: збірник тез Всеукраїнського круглого столу, 15 березня 2024 року. Львів: ЛьвДУВС, 2024. С. 188-197.

249. У Китаї камера розпізнала підозрюваного серед 60 тисяч людей 14 Квітня 2018. URL: https://volynonline.com/u-kitayi-kamera-rozpiznala-pidozryuvanogo-sered-60-tisyach-lyudey/ (дата звернення 25.10.2023).

250. У застосунок дія додано документи про освіту 22 березня 2024. URL: https://mon.gov.ua/ua/news/u-zastosunok-diya-dodano-dokumenti-pro-osvitu (дата звернення 25.10.2024).

251. Угода підписника Steam URL: https://store.steampowered.com/subscriber_agreement/ (дата звернення 05.10.2023).

252. Умови надання послуг Facebook. URL: https://www.facebook.com/legal/terms (дата звернення 12.10.2023).

253. Умови надання послуг TikTok. URL: https://www.tiktok.com/legal/page/us/terms-of-service/uk (дата звернення 12.10.2023).

254. Умови використання. Instagram. URL: https://help.instagram. com/581066165581870/?helpref=uf_share (дата звернення 25.10.2024).

255. Устименко О.А. Індивідуалізація фізичної особи в сучасному світі. *Матеріали Норвезько-української конференції, присвяченої діяльності Ф. Нансена в Україні у 1921–1922 роках,* (Харків, 10–11 жовт. 2019 р.) Х.: ХНУ ім. В.Н. Каразіна, 2019. URL: https:// ekhnuir.karazin.ua/ handle/ 123456789/ 15065 (дата звернення 23.04.2023).

256. Ухвала Верховного Суду України м. Київ у справі № 925/200/22 від 8 лютого 2024 р. URL: https:// reyestr.court.gov.ua/Review/ 116984639?fbclid=PAZXh0bgNhZW0CMTEAAaZET m8i8TWZ4 TZUFn FAB gudJKaBHi wLEldxztiyCeFp7 fSD5l6dJe9xfg4_aem _2nVsd4hie7Vblpx UXmm 9VA# (дата звернення 25.10.2024).

257. Фельдман пропонує прирівняти право на доступ до Інтернету до базових прав людини в Україні. 17.04.2014. URL: https://lb.ua/news/2014/04/17/263469_feldman_predlagaet_priravnyat.html (дата звернення 25.11.2022).

258. Філоненко О. Мають мільйони підписників: як виглядають “блогери”, яких створив штучний інтелект. 5.12.2023. URL: https://life.24tv.ua/blogeri-yakih-stvoriv-shtuchniy-intelekt-yak-viglyadayut-tsi_n2446113 (дата звернення 25.10.2023).

259. Фуко М. Наглядати й карати: Народження в’язниці; пер. з фр. П. Таращук. Київ: Основи, 1998. 392 с.

260. Facebook створив власний Верховний Суд: чим він займається. 08.05.2020. https://loyer.com.ua/uk/facebook-stvoryv-vlasnyj-verhovnyj-sud-chym-vin-zajmayetsya/ (дата звернення 15.10.2023).

261. Харитонов Є.О. «Особа» та «Особистість» – віднайдення парадигми: (цивілістично-теоретичний дискурс за участі М. П. Орзіха). *Часопис цивілістики.* 2017. № 22. С. 140-144.

262. Харитонова О. І. Дещо про стимулякри і нову реальність. Цивілістика в інформаційному суспільстві : матеріали Всеукр. кругл. столу (м. Одеса, 17 трав. 2019 р.) / За заг. ред. д.ю.н., проф. Є. О. Харитонова. Одеса: Фенікс, 2019. С. 8-11.

263. Харитонова О.І., Харитонов Є.О. Віртуальний світ, віртуальна особистість і симулякри. Цифрова трансформація та цифрова економіка в умовах воєнного стану: аспекти інтелектуальної власності. Збірник матеріалів V Всеукр. наук.-практ. конф. з проблем економіки інтелектуальної власності, 27 травня 2022р., Київ: Науково-дослідний інститут інтелектуальної власності НАПрН України, 2022. С. 220-224.

264. Харитонов Є.О. Харитонова О. І., Римське право як підґрунтя сучасного права Європи. *Актуальні проблеми держави і права*. 2005. № 24. С. 10-17. URL: http://nbuv.gov.ua/UJRN/apdp_2005_24_3

265. Харитонов Є.О., Харитонова О.І. Цифрова людина, цифрова особа та цифрова особистість: до проблеми співвідношення. *Часопис цивілістики.* 2023. № 49. С. 5-13.

266. Хаустова М. Державна політика в сфері прав людини в епоху цифрових трансформацій. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2022. № 69. С. 328-333.

267. Хижняк Є.С. Особливості ідентифікації особи злочинця за допомогою IP-адреси / Є. С Хижняк. *Правове життя сучасної України:* матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.). Одеса: Гельветика, 2020. Т. 3. С. 353-356.

268. Худолій Т.І. Персональні дані в системі особистих немайнових прав фізичних осіб в мережі Інтернет: загальна характеристика. *Актуальні проблеми вітчизняної цивілістики.* 2021. № 4. С. 25-30.

269. Цивільне право України: підручник. 4-е вид., перероб. і доп. У 2 частинах. / За ред. проф. Р.Б. Шишки (кер. авт. кол.), Ч. 1. Загальна. Київ: Видавництво Ліра-К, 2025. 800 с.

270. Цивільне право України: Підручник. В 2-х т / За ред. Є.О. Харитонова, Н.Ю. Голубєвої. Харків: «Одіссей», 2008. Том 1. 832 с.

271. Цифровий двійник зможе випробувати на собі ліки і навіть урятувати вам життя 24.04.2023 URL: https://www.imena.ua/blog/digital-twin-can-test-drugs-and-save-your-life/ (дата звернення 25.10.2023).

272. Чалабієва М.Р. Суд у «смартфоні» як штучний інтелект у правосудді: реалії та перспективи. *Юридичний науковий журнал.* 2021. № 10. С. 94-96.

273. Чванкін С.А. Інформаційні технології у доказуванні в цивільному процесі: теоретичні та практичні аспекти. Дисертація. Одеса. 2021. 498 с.

274. Шевчук О.В. Професійна етика у застосуванні технологій штучного інтелекту учасниками судового процесу. *Проблеми реалізації прав, свобод і законних інтересів суб'єктів права в Україні:* матеріали ІІ Всеукраїнської науково-практичної конференції, м. Київ, 8 жовтня 2024 року / відп. ред. А.Ю. Олійник, Ю. В. Оніщик. Київ: КНУТД, 2024. С. 224-229.

275. Шевчук К. Умєров анонсував введення електронного військового квитка та цифровізацію ВЛК. 7.09.2023. URL: https://meta. ua/uk/news/ politics/86854-umerov-anonsuvav -vvedennya-elektronnogo-viiskovogo-kvitka-ta-tsifrovizatsiyu-vlk/(дата звернення 25.10.2023).

276. Шеляженко Ю.В. Правові основи особистої автономії приватних осіб та організацій: теоретичний аспект. Дисертація на здобуття ступеня доктора філософії за спеціальністю. Київ. 2021. 261с.

277. Шишка Р.Б. Охорона прав суб'єктів інтелектуальної власності у цивільному праві України: автореф. дисератції д-октора юрид. наук. Харків, 2004. 37 с.

278. Шишка Р.Б. Індивідуалізація фізичних осіб та рівність. Правове життя сучасної України: матер. Міжнар. наук.-практ. конф. / відп. ред. Г. О. Ульянова. Одеса: ВД «Гельветика», 2019. Т. 2. С. 565-569.

279. Шишка Р.Б. Індивідуалізація людини в умовах інформаційного суспільства. *Legal Bulletin.* 2020. № 1. С. 49-57.

280. Шварк К. У США через 14 років знайшли ґвалтівника: допомогли завантажені ним у мережу результати ДНК-тестів 30.06.21 URL: https://www.unian.ua/world/u-ssha-cherez-14-rokiv-znayshli-gvaltivnika-dopomogli-zavantazheni-nim-u-merezhu-rezultati-dnk-testiv-novini-svitu-11466913.html/ (дата звернення 20.12.2023).

281. Швидка Т., Ніколенко А., Законодавче закріплення права на доступ до Інтернету. *Підприємництво господарство і право.* 2021. № 5. С. 145-150.

282. Шкабаро В.М., Тодорашко Т.А., Біла А.В. Поняття ділової репутації в мережі інтернет: проблеми визначення в законодавстві України. *Вісник університету імені Альфреда Нобеля. серія Право*. 2021. № 1 (2). С. 78-82.

283. "Штучний інтелект" допоможе виявляти тих, хто отримує соціальну підтримку незаконно. 2019. URL: https://life.pravda.com.ua/press-release/2019/07/15/237546/ (дата звернення 20.12.2023).

284. Юридична енциклопедія. В 6 т. / Редкол.: Ю. С. Шемшученко (відп.ред.) та інші. К.:Укр. енцикл., 1998. Т. 1. С. 23.

285. Ямненко Т.М., Місько Д.О. Розвиток цифрових прав в Україні. *Юридичний вісник.* 2022. № 4 (65). С. 101-106.

286. Як цифровий двійник може підвищити ефективність складу? 23 травня 2023 URL: https://haski.ua/blog/chto-takoe-czyfrovыe-dvojnyky-y-kak-ony-mogut-povыsyt-эffektyvnost-sklada (дата звернення 07.09.2023).

287. Як Google використовує файли cookie. Умови конфіденційності. URL: https:// policies. google. com/ technologies/ cookies ?hl=uk (дата звернення 07.09.2023).

288. 10 мільярдів фото і система розпізнавання: Україна отримала доступ до бази Clearview AI. 14.03.2022. URL: https:// www. ukrinform.ua /rubric-

technology/ 3429032-10-milardiv-foto-i-sistema- rozpiznavanna-ukraina- otrimala-dostup-do- bazi-clearview-ai.html (дата звернення 20.11.2022).

289. II Business & Legal It Forum: «Найімовірніше, штучний інтелект буде розглядатися як джерело підвищеної небезпеки» – Майданик Р. 05.10.2022. URL: https:// pravo.ua/ ii-business-legal-it- forum-shvydshe-za-vse-shtuchnyi-intelekt-bude-rozhliadatysia-iak-dzherelo-pidvyshchenoi-nebezpeky-roman-maidanyk/ (дата звернення 20.10.2023).

290. 中文互联网正在加速崩塌 *2024-05-22*. URL: https://web. archive.org/ web/ 202 405 23001 943/https:/mp. weixin.qq.com/s/af g3zHPpEyR zSfO R1Aeh3w (дата звернення 07.11.2024).

291. 关于进一步压实网站平台信息内容管理主体责任的意见 URL: http:// www.gov. cn/zhengce /zhengceku /2021-09/16/content _5637727.htm (дата звернення 07.11.2024).

292. A Blueprint for Digital Identity The Role of Financial Institutions in Building Digital Identity August 2006. URL: https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf (дата звернення 17.11.2022).

293. A guide to data security. Information Comissioer's Office UK. URL**:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/(дата звернення 14.12.2022).

294. A Declaration of the Independence of Cyberspace. URL: https://www.eff.org/cyberspace-independence (дата звернення 20.11.2022).

295. Agrawal A., Horton J., Lacetera N., Lyons E. Digitization and the Contract Labor Market: A Research Agenda. Working paper. Conference June 6–7, 2013. 2015. P. 219-250. URL: https://www.nber.org/ papers/w19525 (дата звернення 17.11.2023).

296. Alexander S.G. Self-sovereign identity. What is self-sovereign identity? 29.12.2022. URL: https://www.techtarget.com/searchsecurity/definition/self-sovereign-identity (дата звернення 20.02.2023).

297. Altman I. The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding. – Monterey, California: Brooks/Cole Publishing Company. 1975. 237 p.

298. Algorithmic Accountability Act of USA. 03.02.2022 S.3572. URL: https:// www.congress. gov/bill/117th-congress/senate-bill/3572/text (дата звернення 17.01.2023).

299. Albrezzi F. Visiting Digital Tombstones: Unearthing Questions of Digital Personhood, Commemoration and Remembrance Processes. A thesis for the degree of Master of Arts in Culture & Performance Studies. Los Angeles, 2015. 55 p.

300. Access Now. KeepitOn campaign. January 29, 2020. https://www.accessnow.org/ keepiton/ (дата звернення 17.11.2022).

301. Access intervenes at ECtHR for the right to be anonymous online. June, 2014.URL: https://www.accessnow.org/access-intervenes-at-ecthr-for-the- right-to-be-anonymous -online. (дата звернення 17.01.2023).

302. A comprehensive approach on personal data protection in the European Union. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. Brussels. 4.11.2010. URL: https://eur-lex.europa.eu/ legal-content/EN/TXT/HTML/ ?uri= CELEX:52010DC0609&from=FR/ (дата звернення 25.10.2022).

303. A Digital Mausoleum: Facebook After Death February. 13, 2015. URL: https://www.wnycstudios.org/podcasts/takeaway/segments/new-facebook-policy-lets-you-decide-what-happens-your-profile-when-you-die /(дата звернення 17.11.2022).

304. A new way for families to make purchases on Google Play. December 20, 2022. URL: https://blog.google /products/google-play/purchase-requests- google-play-families/ (дата звернення 17.11.2023).

305. Alarm over China’s disappearing online content. 27.05.2024. URL: https://www.ucanews.com/ news/alarm-over-chinas- disappearing-online-content/105221 (дата звернення 17.11.2024).

306. Al-Majid W. Electronic Agents and Legal Personality: Time to Treat Them as Human Beings. Annual Conference, Herftordshire, 16-17 April, 2007. URL:

http://www.bileta.ac.uk /Document%20Library /1/Electronic%20Agents %20and%20Legal%20 Personality%20- %20Time% 20to%20Treat %20Them%20as%20Human%20Beings.pdf (дата звернення 17.11.2022).

307. Allan T., Widdison R. Can Computers Make Contracts? *Harvard Journal of Law & Technology*. 1996. № 1. Vol. 9. P. 25-52. URL: http://jolt.law.harvard.edu/volumes/volume-9 (дата звернення 17.11.2022).

308. An Introduction to Online Platforms and their Role in Digital Transformation 2019. OECD. URL: https://www.oecd.org/innovation/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation-53e5f593-en.htm (дата звернення 17.02.2024).

309. Analytical report on EU law applicable to sharing of non-personal data. Support Centre for data sharingSmart 2018/1009. 2020. Vol.2.0. 65 p. URL: https://data.europa.eu/sites/default/files/course/EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf (дата звернення 17.11.2022).

310. Angwin J., Larson J., Mattu S., Kirchner L. Machine Bias, May 23, 2016 URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (дата звернення 17.11.2022).

311. D'Amato A., Chopra S. K. Whales: Their Emerging Right to Life. *American Journal of International Law.* 1991. № 85 (1). p. 2162. DOI: https://doi.org/10.2307/2203067

312. Are cookies personal data? May 22, 2019. URL: https://usercentrics.com/knowledge-hub/cookies-personal-data/(дата звернення 17.01.2024).

313. Artificial Intelligence Act. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts-2021/0106(COD) URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf(дата звернення 17.11.2024).

314. Artificial intelligence: How does it work, why does it matter, and what can we do about it? 28 June, 2020. URL: https://www.europarl. europa.eu/ stoa/en/ document/ EPRS_STU(2020)641547 (дата звернення 17.08.2022).

315. Ashbourn J. Identification, verification and templates. In: Biometrics: Advanced Identity Verification. Springer, London. 2000. P. 59-61. URL: https://doi.org/10.1007/978-1-4471-0747-7_4

316. Ashley K.D. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age, Cambridge University Press, 2017. 640p. URL: https://doi.org/10.1017/9781316761380 (дата звернення 17.09.2022).

317. Autoriteit Persoonsgegevens 4 december 2019. Besluit tot het opleggen van een bestuurlijke boete URL: https://autoriteitpersoonsgegevens.nl/uploads/imported/boetebesluit_vingerafdrukken_personeel.pdf (дата звернення 17.03.2024).

318. Baudrillard J. Simulacra and Simulation (Translated by Sheila Faria Glaser). University of Michigan Press. 1994 164 p.

319. Bachelet M. Artificial intelligence risks to privacy demand urgent action. 15 September, 2021. URL: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E (дата звернення 20.11.2023).

320. Back M.D., Stopfer J.M., Vazire S., Gaddis S., Schmukle S. C., Egloff B., Gosling S.D. Facebook Profiles Reflect Actual Personality, Not Self-Idealization. *Psychological Science.* 2010. № 3. P. 372-374.

321. Balkin J.M. The Path of Robotics Law. *California Law Review*. 2015. № 536. URL: https://ssrn.com/abstract=2586570 (дата звернення 17.11.2023).

322. Balkin J.M. The Three Laws of Robotics in the Age of Big Data. *Ohio state Law Journal.* 2017. № 78. URL: https:// firstmonday .org/ojs/ index.php /fm/ article/ view/7113 (дата звернення 17.11.2023).

323. Banteka N. A Network Theory Approach to Global Legislative Action. *Seton Hall Law Review.* 2020. № 2. P. 340-399. URL: https://ssrn. com/abstract =3573175 (дата звернення 17.05.2023).

324. Ban dangerous facial recognition technology that amplifies racist policing. January 26, 2021 URL: https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/ (дата звернення 17.11.2022).

325. Barbaro M., Zeller J.T. A Face Is Exposed for AOL Searcher № 4417749. Aug. 9, 2006. URL: https://www.nytimes.com/2006/08/09/technology/09aol.html(дата звернення 07.11.2023).

326. Barricelli B.R., Casiraghi E., Gliozzo J., Petrini A., Valtolina S. Human digital twin for fitness management. *IEEE.* 2020. № 8. https://doi.org/10.1109/ACCESS.2020.2971576(дата звернення 17.05.2023).

327. Barlow J.P. A Declaration of the Independence of Cyberspace. *Duke Law & Technology Review.* 2019. Vol. 18. № 1. P. 5-7. URL: https://scholarship.law.duke.edu/dltr/vol18/iss1/2 (дата звернення 18.05.2023).

328. Barrat A. et al., *The Architecture of Complex Weighted Networks*. National academy of sciences. 2004. №101. P. 3747-3752. DOI:10.1073/pnas.0400087101. (дата звернення 17.11.2024).

329. Basu T. This couple just got married in the Taco Bell metaverse. *MIT Technology Review.* URL: https:// www.technologyreview.com /2023/03/15/1069848/ taco-bell-metaverse-wedding/ (дата звернення 17.11.2024).

330. Bayer J., Bitiukova N., Bard P. Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States European Parliament, LIBE Committee, Policy Department for Citizens' Rights and Constitutional Affairs. February 1, 2019. URL: https://ssrn. com/abstract =34092 79(дата звернення 17.11.2023).

331. Bernstein, Lisa E. Contract Governance in Small World Networks: The Case of the Maghribi Traders. *Northwestern University Law Review.* 2018. № 5 (113). P. 1009-1070. URL: https://ssrn.com/abstract=3278003 (дата звернення 17.11.2024).

332. Bingham T. The rule of law The Sixth Sir David Williams Lecture. 2006. URL: https://www. cpl.law.cam.ac.uk/sites/www.law. cam.ac.uk/files/images/

www.cpl.law.cam.ac.uk/ legacy/ Media/ THE%20RULE%20OF%20LAW%202006.pdf (дата звернення 17.03.2023).

333. Birch D. Blockchain Digital ID – Putting People in Control of Their Data. 2020. URL: https://cointelegraph.com/news/blockchain-digital-id-putting-people-in-control-of-their-data (дата звернення 15.05.2023).

334. Being Your Authentic Self on Facebook. URL: https://www.facebook.com/help/186614050293763/?helpref=hc_fnav (дата звернення 15.05.2024).

335. Bernard A. La protection de l'intimité par la droit privé: eloge du ragot ou comment vices exposes engendrent vertu. *Les For Interieur*. P. 153-179. URL: https://extra.u-picardie.fr/ outilscurapp/medias/revues/35/ alain_bernard.pdf _4a081e8ad4544/alain_bernard.pdf (дата звернення 15.05.2024).

336. Benedek W., Kettemann M. Freedom of Expression and the internet. Updated and revised 2nd edition, Council of Europe Publishing, December 2020, 235 p.

337. Benvenuti S, Zolea S. European courts and predictive justice: a feasible symbiosis? *Opinio Juris in Comparatione*. 2023. Vol. 1. № 1. P. 54-89. URL: https:// www. opiniojurisincomparatione.org/ wp-content/uploads /2023/12/Opinio _Template-Zolea. pdf (дата звернення 15.01.2024).

338. Best M. Can the Internet be a Human Right? *Human Rights & Human Welfare*. 2004. № 1 (4). P. 23-31. URL: https:// digitalcommons.du. edu/hrhw/ vol4/i ss1/13/ (дата звернення 15.05.2024).

339. Blackman J. Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet. *Santa Clara Law Review.* 2008. № 49. P. 313-392. URL: https://ssrn.com/abstract=1116776 (дата звернення 15.02.2024).

340. Blaschke Y. Digital rights as a security objective: New gateways for attacks. URL: https://edri.org/our-work/digital-rights-as-a-security-objective-new-gateways-for-attacks/ (дата звернення 15.05.2023).

341. Bogdanowivz M., Beslay I. Cyber-security and the future of identity. IPTS report, September, 2002. URL: http://_www.jrc. es/ home/report/ english/ articles/ vol57/ ICT4E576.htm (дата звернення 15.05.2024).

342. Bond S. AI fakes raise election risks as lawmakers and tech companies scramble to catch up. February 8, 2024. URL: https:// www.npr.org/ 2024/02/ 08/ 1229641751 /ai-deepfakes-election-risks-l awmakers-tech-companies- artificial-intelligence (дата звернення 15.11.2024).

343. Bosani E. European digital identity, all personal documents in one app. June 9, 2021. URL: https://www.egalite.org/identita-digitale-europea/ (дата звернення 15.05.2022).

344. Bosco F., Creemers N., Ferraris V. et al Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. S. Gutwirth, R. Leenes, P. de Hert (eds.). *Reforming European Data Protection Law*. 2014. P. 3-33. URL: https://doi.org/10.1007/978-94-017-9385-8_1(дата звернення 15.05.2023).

345. Bostrom N., Yudkowsky E. The Ethics of Artificial Intelligence. Artificial Intelligence Safety and Security. ed. by R. V. Yampolskiy. New York: Routledge, 2018. P. 57-69.

346. Bozdag E. Bias in Algorithmic Filtering and Personalization. *Ethics and Information Technology.* 2013. Vol. 15. P. 209-227. URL: http://DOI 10.1007/s10676-013-9321-6

347. Bradford A. The Brussels Effect. *Nortwestern University Law Review*. 2012. № 1. P. 1-68. URL: https:// scholarship. law.columbia. edu/ faculty_scholarship /271. (дата звернення 15.05.2023).

348. Brenner S., Zarnekow W., Wittig H. Intelligente Softwareagenten: Grundlagen und Anwendungen, Berlin. 1998. 371p.

349. Brewster T. Fraudsters Cloned Company Director’s Voice In $35 Million Heist, Police Find. *Forbes*. 2021. URL: https://www.forbes.com/ sites/thomasbrewster/2021/10/14/ huge- bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=6409fbc87559 (дата звернення 12.05.2022).

350. Brownsword R., Goodwin M. Law and the Technologies of the Twenty-First Century. Cambridge University Press. 2012. 469 p. URL: https://www.cambridge.org/core/books/law-and-the-technologies-of-the-twentyfirst-century/996EC2CB971505916B78C0F299A17BF2 (дата звернення 15.05.2022).

351. Brudbaker J.R. Death, Identity and the Social Network: Dissertation for the degree of Doctor of Philosophy. Irvine, 2015. 278 p. URL: https://escholarship.org/content/qt6cn0s1xd/qt6cn0s1xd_ noSplash_20 00bf31aa1dd 63c58e270c2154ae30d.pdf (дата звернення 19.05.2022).

352. Buchanan I. Deleuze and the Internet. *Australian Humanities Review*. 2007. № 43. P. 1-19. URL: https://ro.uow.edu.au/artspapers/1392 (дата звернення 15.05.2023).

353. Buitelaar J.C. Post-mortem privacy and informational self-determination. *Ethics and Information Technology*. 2017. № 2.Vol. 19. P. 129-142.

354. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Herrn Gunther Frhr.v. M. Dec. 15, 1983. URL: http://www.servat.unibe.ch/dfr/bv065001.html(дата звернення 12.07.2023).

355. Bundesgesetz, mit dem Arbeiten mit gentechnisch veränderten Organismen, das Freisetzen und Inverkehrbringen von gentechnisch veränderten Organismen und die Anwendung von Genanalyse und Gentherapie am Menschen geregelt warden (GTG) StF: BGBl. Nr. 510/1994. [The Legal Information System of the Republic of Austria]. URL: https:// www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer =10010826 (дата звернення 18.07.2023).

356. Bundesgerichtshof BGH, Beschluss vom 27. August 2020 - III ZB 30/20 - KG Berlin. URL: https:// juris.bundesgerichtshof. de/cgi-bin/rechtsprechung/document.py?Gericht=bgh& Art=en&nr=110132 &pos= 0& anz =1 (дата звернення 15.05.2023).

357. Byrnes N. Why We Should Expect Algorithms to Be Biased. 2016. URL: https://www.technologyreview.com/2016/06/24/159118/why-we-should-expect-algorithms-to-be-biased/ (дата звернення 15.12.2022).

358. Burt C. Digital identity market to reach $33B in 2025, Malaysia plans biometric national online ID system Jul 27, 2020. URL: https://www.biometricupdate.com/202007/digital-identity-market-to-reach-33b-in-2025-malaysia-plans-biometric-national-online-id-system_____(дата звернення 15.02.2023).

359. Cahn N.R. Probate Law Meets the Digital Age. *Vanderbilt Law Review*. 2014. Vol. 67. P. 1697-1727. URL: https://scholarship.law.vanderbilt.edu/vlr/vol67/iss6/7/ (дата звернення 15.12.2023).

360. Callamard A. The Human Rights Obligations of Non-State Actors. In *Human Rights in the Age of Platforms* edited by Rikke F. Jørgensen: Cambridge, MA: MIT Press, 2019. P. 191-225.

361. Cali B. The Case for the Right to Meaningful Access to the Internet as a Human Right in International Law. *A. von Arnauld The Cambridge Handbook of New Human Rights*, Cambridge University Press, January 2020. P. 276-284.

362. California Consumer Privacy Act of 2018 URL: https:// leginfo. legislature.ca. gov/faces/codes_displayText. xhtml?division=3.&part=4.&law Code=CIV&title=1.81.5 (дата звернення 15.05.2023).

363. Calo R. Robotics and the Lessons of Cyberlaw. *California Law Review.* 2015. Vol. 103. № 3. P. 513-63. URL: https://ssrn.com/abstract= 2402972 (дата звернення 15.10.2023).

364. Cambridge Analytica Whistleblower, Brittany Kaiser. Oxford Union. URL: https://www.youtube.com/watch?v=AgBHfmf2JhQ (дата звернення 15.10.2023).

365. Canada lawyer under fire for submitting fake cases created by AI chatbot. URL: https://www.theguardian.com/world/2024/feb/29/canada-lawyer-chatgpt-fake-cases-ai (дата звернення 10.12.2024).

366. Daniel C., Palmer M. Google’s Goal: To Organise Your Daily Life. *Financial Times.* May 22, 2007. URL: http://www.ft.com/cms/s/2/c3e49548-088e-11dc-b11e-000b5df10621.html p (дата звернення 15.07.2023).

367. Case of Axel Springer AG v. Germany. (Application no. 39954/08) 7 February 2012. *HUDOC / European Court of Human Rights.* URL: http://hudoc.echr.coe. int/eng?i=001-109034 (дата звернення 10.05.2022).

368. Case of Affaire Hurbain c. Belgique (Application no. 57292/16) 22 Juin 2021. *HUDOC / European Court of Human Rights. URL:* https://hudoc.echr.coe.int/rus#%7B%22itemid%22:%5B%22001-210467%22%5D%7D (дата звернення 10.05.2022).

369. Case of Ahmet Yildirim and others v. Turkey (Application no. 3111/10) 18 December 2012. *HUDOC / European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng?i=001-115705 (дата звернення 10.05.2022).

370. Case of Bank Austria Creditanstalt AG v. Commission of the European Communities Case T-198/03. 30 May 2006. *CJEU / Court of Justice of The European Union.* URL: https://curia.europa.eu/juris/liste.jsf?language=en&num=T-198/03 (дата звернення 10.05.2022).

371. Case of Benedik v. Slovenia (Application no. 62357/14) 24 April 2018. *HUDOC / European Court of Human Rights.* URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-182455%22]} (дата звернення 10.05.2022).

372. Case of Bensaid v. United Kingdom (Application no. 44599/98) 6 May 2001. *HUDOC / European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59206%22]} (дата звернення 10.05.2022).

373. Case of B.B. v. France (Requête no. 5335/06) 17 décembre 2009. *HUDOC / European Court of Human Rights.* URL: https://ips.ligazakon.net/document/ES008449 (дата звернення 10.05.2022).

374. Case of Bodil Lindqvist v. Åklagarkammaren i Jönköping. C-101/01. 6 November 2003. *CJEU / Court of Justice of The European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62001CJ0101(дата звернення 10.05.2022).

375. Case Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH. C 673/17. 1 October 2019. *CJEU / Court of Justice of The European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0005 (дата звернення 10.05.2022).

376. Case of Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni. C-398/15. 9 March 2017. *CJEU / Court of Justice of The European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0398 (дата звернення 10.10.2022).

377. Case of Catt v. the United Kingdom (Application no. 43514/15) 24 January 2019. *HUDOC / European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-189424%22]} (дата звернення 10.10.2022).

378. Case of Dalea v. France (Application no. 964/07) 2 February 2010. *HUDOC / European Court of Human Rights.* URL: *https:// hudoc.echr.coe.int/ eng#{%22itemid%22: [%22002-1119%22]}* (дата звернення 10.10.2022).

379. Case of Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems. C-311/18. *16 July 2020. CJEU / Court of Justice of The European Union.* URL: https:// eur-lex.europa.eu /legal-content/ EN/TXT/ ?uri=CELEX%3A62018CJ0311 (дата звернення 10.10.2022).

380. Case of Delfi AS v. Estonia (Application no. 64569/09). 10 October 2013. *HUDOC / European Court of Human Rights*. URL: http://www.statewatch.org/news/2013/oct/echr- judgment-delfi-AS-v-estonia.pdf (дата звернення 10.10.2022).

381. Case of Gardel v. France (Application no. 16428/05) 17 March 2010. *HUDOC / European Court of Human Rights*. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-96457%22]} (дата звернення 10.10.2022).

382. Case of Gaughran v. the United Kingdom (Application no. 45245/15) 13 February 2020. *HUDOC / European Court of Human Rights.* URL:

https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-200817%22]} (дата звернення 10.10.2022).

383. Case of Gill v. Hearst Pub. Co., Inc. February 17, 1953. California Supreme Court. URL: https: //case-law. vlex.com /vid/gill-v-hearst-pub-895214654 (дата звернення 10.10.2022).

384. Case of Graham Gaskin v. the United Kingdom. (Application no.10454/83) 13 November 1987. HUDOC / *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-45386%22]} (дата звернення 10.10.2022).

385. Case of Grainger Plc and others v. Nicholson 2009. UKEAT/0219/09. United Kingdom Employment Appeal Tribunal. 7 October 2009. URL: https:// ww w.bailii.org/uk /cases/ UKEAT/2009/0219_09_0311.html (дата звернення 10.10.2022).

386. Case of Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. C-131/12. 13 May 2014. *CJEU / Court of Justice of The European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131 (дата звернення 10.10.2022).

387. Case of Godelli v. Italy (Application no. 33783/09) 18 March 2013. HUDOC / *European Court of Human Rights.* URL: https:// hudoc.echr.coe.int/ eng#{%22itemid%22:[%22001-113460%22]} (дата звернення 11.10.2022).

388. Case of Heinz Huber v. Bundesrepublik Deutschland. C-524/06. 18 December 2008. *CJEU / Court of Justice of The European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62006CJ0524 (дата звернення 11.10.2022).

389. Case of Jankovskis v. Lithuania (Application no. 21575/08) 7 April 2017. HUDOC / *European Court of Human Rights.* URL: https:/ /hudoc.echr.coe. int/fre#{%22itemid%22:[%22001-170354%22]} (дата звернення 10.12.2022).

390. Case of Kalda v. Estonia (Application no. 17429/10) 19 January 2016. HUDOC / *European Court of Human Rights.* URL: https:// hudoc.echr. coe.int/eng#{%22itemid%22: [%22001-160270%22]} (дата звернення 10.12.2022).

391. Case of Kalkar I. 8 August 1978. *BverfGE / Entscheidungen des Bundesverfassungsgerichts.* URL: https://openjur.de/u/166332-quotes.html (дата звернення 11.10.2022).

392. Case of Leander v. Sweden (Application no. 9258/81) 26 March 1987. HUDOC / *European Court of Human Rights.* URL: https:// hudoc.echr. coe.int/eng# {%22itemid%22:[%22001-57519%22]} (дата звернення 10.01.2023).

393. Case of Marianne Ajemian & another v. Yahoo!, Inc. 9 March 2017. SJC–12237. Supreme Judicial Court of Massachusetts, Norfolk. URL: https: //case-law. vlex. com/ vid/ajemian-v-yahoo-inc- 886625134?_ gl=1*47jwkk*_ up*MQ..*_ga*NTg2MDQy MjU4LjE3N TEwMjE1MjI.*_ga_ VZEM72P2C6 *czE3NTEwMjE 1MjEkbzEkZzEkdDE 3NTEwMjE 1MzckajQ0 JGwwJGgw (дата звернення 10.02.2023).

394. Case of Michael A. Clausen v. Beneficial Finance Company of Berkeley. July 20, 1976. URL: https:// law.justia.com/ cases/federal/ district-courts/FSupp/ 423/985/ 2393237/ (дата звернення 15.11.2022).

395. Case of Mikulić v. Croatia (Application no. 53176/99) 7 February 2002. *HUDOC / European Court of Human Rights. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-60035%22]}* (дата звернення 10.10.2022).

396. Case of ML & WW v. Germany (Applictions No. 60798/10 and 65599/10) 28 June 2018. *HUDOC / European Court of Human Rights*. URL: https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001-183947&filename=CASE%20OF%20M.L.%20AND%20W.W.%20v.%20GERMANY.pdf (дата звернення 10.10.2022).

397. Case of M.M. v. the United Kingdom (Application no. 24029/07) 13 November 2012. HUDOC / *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-114517%22]} (дата звернення 10.02.2023).

398. Case of Niemietz v. Germany (Application no. 13710/88) 16 December 1992. HUDOC / *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng?i=001-57887 (дата звернення 10.02.2023).

399. Case of *Odievre v. France* (Application no. № 42326/98) 13 February *2003.* HUDOC / *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-60935%22]} (дата звернення 10.03.2023).

400. Case of PG and JH v. The United Kingdom (Application no 44787/98) 25 September 2001. HUDOC / *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59665%22]} (дата звернення 10.05.2023).

401. Case of Peck v. United Kingdom (Application no. 44647/98) 28 January 2003. HUDOC / *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-60898%22]} (дата звернення 10.02.2023).

402. Case of Perry v. the United Kingdom (Application no. 63737/00) 17 October 2003. HUDOC / *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-61228%22]} (дата звернення 12.05.2023).

403. Case of Peter Nowak v. Data Protection Commissioner (Application: OJ C 364 from 03.10.2016) 20 December 2017. *CJEU / Court of Justice of The European Union.* URL: https://curia.europa. eu/juris/document/ document.jsf?text= &docid=198059 &pageIndex=0&doclang=en&mode=lst&dir= &occ=first&part= 1&cid= 14552558 (дата звернення 10.05.2023).

404. Case of R (on the application of Edward BRIDGES) v. The Chief Constable of South Wales Police. No C1/2019/2670. 11 August 2020. The Court of Appeal Cardiff District Registry. URL: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf (дата звернення 12.05.2023).

405. Case of Rasmussen v. Denmark (application no. 8777/79) 28 November 1984. HUDOC / *European Court of Human Rights.* URL: https: //ips .ligazakon. net/document/ ES012478 (дата звернення 14.05.2023).

406. Case Rees v. The United Kingdom *(Application no. 9532/81)* October 1986. HUDOC / *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-57564&filename=CASE%20OF%20REES%20v.%20THE%20UNITED%20KINGDOM.docx&logEvent=Fa (дата звернення 14.05.2023).

407. Case of Relu Adrian Coman and Others v. Inspectoratul General pentru Imigrări and Ministerul Afacerilor Internet, 5 June 2018 № C-673/16. *CJEU / Court of Justice of The European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0673 (дата звернення 14.04.2023).

408. Case of S. and Marper v. the United Kingdom (Application no. 30562/04) 4 December 2008. HUDOC / *European Court of Human Rights.* URL: https: //hudoc. echr.coe.int/fre#%7B%22itemid%22:[%22001-90051%22]%7D (дата звернення 10.03.2023).

409. Case of Schrems M. v Data Protection Commissioner, Digital Rights Ireland Ltd. C-362/14. 6 October 2015. *CJEU / Court of Justice of The European Union.* URL: https://curia. europa.eu/juris/ document/ document. jsf?text=&docid=169195&pageIndex= 0&doclang= EN&mode=req&dir=&occ=first&part=1&cid=143358 (дата звернення 10.03.2023).

410. Case of State Farm Mutual Automobile Insurance Company, Acorporation, Plaintiff-appellant, v. Alfred E. Bockhorst et al., Defendant-appellee. January 14, 1972. URL: https://case-law.vlex.com/vid/state-farm-mutual-automobile-884590067 (дата звернення 10.04.2023).

411. Case of Szabó and Vissy v. Hungary (Application no. 37138/14) 12 January 2016. *HUDOC / European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160020%22]} (дата звернення 10.03.2023).

412. Case of Thaler (Appellant) v. Comptroller-General of Patents, Designs and Trade Marks (Respondent) 2023 UKSC 49. URL: https://supremecourt.uk/uploads/uksc_2021_0201_press_summary_b736b90ccf.pdf (дата звернення 10.06.2024).

413. Case of T & Anor, R (on the application of) v. Secretary of State for the Home Department & Anor. UKSC 35. 18 June 2014. URL: *http://www.bailii.org/uk/cases/UKSC/2014/35.html* (дата звернення 08.05.2023).

414. Case of Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'. C-13/16. 4 May 2017. *CJEU / Court of Justice of The European Union.* URL: https://curia.europa.eu/juris/liste.jsf?num=C-13/16 (дата звернення 10.10.2023).

415. Case of Von Hannover v. Germany (Applications nos. 40660/08 and 60641/08) 7 February 2012. *HUDOC / European Court of Human Rights.* URL: https:// www.abbro-bg.org/ wp-content/uploads/ 2019/09/ CASE-OF-VON-HANNOVER-v.-GERMANY-No.-2.pdf (дата звернення 11.06.2023).

416. Case of Z v. Finland (Application no. 22009/93) 25 February 1997. HUDOC / *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-9432%22]} (дата звернення 11.06.2023).

417. Case of State of Wisconsin v. Eric L. Loomis. July 13, 2016 № 2015AP157-CR URL: https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html (дата звернення 12.07.2023).

418. Castells M. Communication, Power and Counter-power in the Network Society. International Journal of Communication. 2007. №1. P. 238-266.

419. Castronova E. Theory of the avatar. CESIFO Working Paper. 2003. № 863. P.1-45. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=385103 (дата звернення 15.03.2023).

420. Cavoukian A. Privacy by Design The 7 Foundational Principles. URL: https:// privacy.ucsc.edu/ resources/privacy-by- design---foundational-principles.pdf (дата звернення 17.05.2023).

421. Cerf V. Internet Access is Not a Human Right. URL: https://www.nytimes. com/2012/01/05/opinion/ internet-access-is-not-a-human-right. html?_ r=2&pagewanted=all (дата звернення 18.05.2023).

422. Chadwick A., May C. Interaction between States and Citizens in the Age of Internet: “eGovernment” in the United States, Britain and the European Union. *Governance.* 2003. №. 2. V. 16. P. 271-300.

423. Chadwick R., Levitt M., Shickle D. et al., The right to know and the right not to know: Genetic Privacy and Responsibility. [2nd Edition] Cambridge University Press. 2014. 361p.

424. Charter of Digital Fundamental Rights of the European Union. 03 May 2005. URL: https://www. eesc.europa.eu /et/documents/european-digital-charter (дата звернення 18.03.2023).

425. Carpenter C. His body, his choice: pitching infant male circumcision to health and human rights gatekeepers. In: Carpenter C (ed.) *“Lost” causes: agenda vetting in global issue networks and the shaping of human security*. Ithaca. NY: Cornell University Press, 2014. P. 122-147. URL: https://doi.org/10.7591/cornell/9780801448850.003.0006

426. Charter of fundamental rights of the European Union. OJ C 364, 18.12.2000. Official Journal of the European Communities. P. 1-22. URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf (дата звернення 18.06.2023).

427. Chen D.L. Machine Learning and the Rule of Law. Law as Data, Santa Fe Institute Press, ed. M. Livermore and D. Rockmore, 2019. № 16. P. 1-12. URL: https://ssrn.com/abstract=3302507 (дата звернення 10.08.2023).

428. Chomba-Kinywa P. Digital Rights: Why we deserve a free and fair Internet. TEDxLusakaStudio URL: https://www.youtube. com/watch? app=desktop &v=Ppv4PkBjRE8 (дата звернення 10.05.2023).

429. Chopra S., White L. Artificial Agents – Personhood in Law and Philosophy. Brooklyn College. URL: http://www.sci.brooklyn.cuny. edu/~schopra/agentlawsub.pdf. (дата звернення 13.08.2023).

430. Christensen C.M., Raynor M.E., McDonald R. What is Disruptive Innovation? *Harvard Business Review,* 2015. № 12(93). P. 44-53.

431. Citron D.K. Technological due process. *Washington University Law Review.* 2007. № 6. 1249-1313.

432. Citron D.K., Pasquale F.A. The scored society: Due process for automated predictions. *Washington Law Review.* 2014. № 89. P. 1-34.URL: https://ssrn.com/abstract=2376209 (дата звернення 12.07.2023).

433. Civil Court of the City of New York, McEvans v. Citibank N.A. New York City Court. 27 July 1978. URL: https: //case-law. vlex.com/ vid/mcevans-v-citibank-n-884429573 (дата звернення 18.07.2023).

434. Clarke R.A. Profiling: A Hidden Challenge to the Regulation of Data Surveillance. *Journal of Law & Information Scince.* 1993. № 4 (2). URL: http://www.rogerclarke.com/DV/PaperProfiling.html (дата звернення 19.07.2023).

435. Clarke R. What's 'Privacy'? URL: http://www. rogerclarke. com/DV/ Privacy. html (дата звернення 12.07.2023).

436. Clarke R.A. iHuman Identification in Information Systems: Management Challenges and Public Policy. *Information Technology & People*. 1994. № 7 (4). P. 1-36. URL: http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html. (дата звернення 15.07.2023).

437. Coccoli J. The Challenges of New Technologies in the Implementation of Human Rights: An Analysis of Some Critical Issues in the Digital Era. *Peace Human Rights Governance*. 2017. № 2. P. 223-250. DOI: 10.14658/PUPJ-PHRG-2017-2-4 (дата звернення 15.07.2023).

438. Code of EU online rights. European Commission. 17.12.2012. URL: https://doi.org/10.2759/8899 (дата звернення 12.07.2023).

439. Committee On network science for future army applications et al., Network Science.Washington, D.C.: The National Academies Press. 2005 108p. URL: https://nap.nationalacademies.org/read/11516/chapter/1(дата звернення 19.07.2023).

440. Commission proposes a trusted and secure Digital Identity for all Europeans Brussels, 3 June 2021

https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663(дата звернення 17.07.2023).

441. Compilation of Patient Protection and Affordable Care Act [As Amended Through May 1, 2010] http://housedocs.house.gov/energycommerce/ppacacon.pdf (дата звернення 12.07.2023).

442. Constitution of the Portuguese Republic. 2 April 1976. URL: https://diariodarepublica.pt/dr/geral/en/relevant-legislation/constitution-of-the-portuguese-republic_(дата звернення 13.08.2023).

443. Convention on the Rights of the Child. 20 November 1989. General Assembly resolution 44/25. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (дата звернення 14.08.2023).

444. Coupland D. Life After God. New York: Pocket Books, 1994. 368 p.

445. Crawford S.P. Who's in Charge of Who I Am? Identity and Law Online. *New York Law School Law Review.* 2004. № 130 (49). P. 1-14. URL: https://ssrn.com/abstract=796844 (дата звернення 12.07.2023).

446. Cresswell M., Worth A., Sheikh A. Actor-Network Theory and its role in understanding the implementation of information technology developments in healthcare. *BMC Medical Informatics and Decision Making.* 2010. № 10. URL: https://doi.org/10.1186/1472-6947-10-67 (дата звернення 12.07.2023).

447. Custers B. New digital rights: Imagining additional fundamental rights for the digital era. *Computer law & security review.* 2022. № 44. P. 1-13. URL: https://doi.org/10.1016/j.clsr.2021.105636.

448. Custers B., Calders T. What Is Data Mining and How Does It Work? In: Custers B. Calders T., Schermer B., Zarsky T. Discrimination and Privacy in the Information Society. Springer. 2013. P. 1-42. URL: https:// ssrn.com/ abstract=3047758(дата звернення 08.07.2023).

449. Cyphers B., Schwartz A., Sheard N. Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-time Tracking, and More. October 7, 2021. URL:

https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification (дата звернення 08.07.2023).

450. Steinbock D.J. Data Matching, Data Mining, and Due Process. *Georgia Law Review.* 2005. P. 1-86. URL: https:// ssrn.com/ abstract=763504 (дата звернення 15.07.2023).

451. Data protection law: Approaching its rationale, logic and limit by L.A. Bygrave. The Hague: Kluwer Law International, 2002. 456p. (дата звернення 14.07.2023).

452. Data Protection Act UK. 2018. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents (дата звернення 15.07.2023).

453. Day T. Avatar Rights in a Constitutionless World. *Hastings communications and entertainment law journal*. 2009. № 1. P. 137-156. URL: https://repository.uchastings.edu/_hastings_comm_ent_law_journal (дата звернення 12.08.2023).

454. Davis P., Schwemer S.F. Rethinking Decisions Under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making. *Proceedings of the Third International Workshop on Artificial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace held in conjunction with ICAIL.* 2023. P. 1-9. URL: https://ssrn.com/abstract=4478107(дата звернення 15.02.2024).

455. Davydova I., Andronov I., Zhurylo S., Zubar V., Illiopol I. Prospects for the use of AI in Jurisprudence: From the Educational process to Legal Practice. The experience of China. *Revista de Tecnología de Información y Comunicación en Educación*. 2023. № 4 P. 87-95. URL: https://doi.org /10.46502/issn.1856-7576/2023.17.04.9 (дата звернення 14.04.2024).

456. Davydova I., Bernaz-Lukavetska O., Tokareva V., Andriienko I., Tserkovna O. Freedom of contract in the digital age and its implementation in modern technologies: theory and practice. *International Journal of Computer Science and Network Security*. 2022. № 12 (21). P. 544-548. URL: http://paper. ijcsns.org /07_book/202112/20211275.pdf (дата звернення 18.07.2023).

457. Davydova, I., Nahnybida V., Adamova O., Zhurylo S., & Tokareva V. Blockchain and civil proceedings: points of convergence. *DIXI*. 2022. № *25*(1). P. 1-20. URL: https://revistas.ucc.edu.co/index.php/di/article/view/4637 _(дата звернення 18.08.2023).

458. Davydova I., Zhurylo S., Tomina V., Fuchedzhi V., Tokareva V. Legal aspects of regulation of relations with the participation of artificial intelligence. *Revista de la Universidad del Zulia*, 2022. № 38. Vol. 13. P. 487-500. URL: https:// produccioncientificaluz.org /index.php/ rluz/article/view/38726/43136 (дата звернення 19.04.2023).

459. David R.J., Post D.G. Law and Borders-The Rise of Law in Cyberspace. *Stanford Law Review.* 1996. № 48. P.1367-1402. URL: https://ssrn.com/abstract=535 (дата звернення 14.08.2023).

460. Davenport T., Prusak L. Working knowledge: Managing what your organization knows. Boston, MA: Harvard Business School Press. 1998. P. 1-15. URL: https:// www.researchgate.net /publication/ 229099904_ Working_ Knowledge _ How_Organizations_Manage_What_They_Know (дата звернення 14.07.2023).

461. D' Acquisto G., Domingo-Ferrer G., etc. Privacy by design in big data. European Union Agency For Network And Information Security. 2015. 80 p. URL: https://op.europa.eu/en/publication-detail/-/publication/20492499-ce2e-11e5-a4b5-01aa75ed71a1/language-en (дата звернення 18.08.2023).

462. De Hingh A.E. Some Reflections on Dignity as an Alternative legal Concept in Data Protection Regulation. *German Law Journal.* 2018. Vol. 19. №. 5. P. 1269-1290. URL: https://research.vu.nl/ ws/ portalfiles/ portal/86722703/ some_ reflections_on_dignity_as_an_alternative_legal_concept_in_data_protection_regulation.pdf (дата звернення 05.07.2023).

463. Deakin S., Markou C. Is law computable?: Critical perspectives on law and artificial intelligence, Bloomsbury Publishing, 2020. 343p. URL: https://_www. scribd.com /document/ 727537644/ Deakin-Simon-y-Markou- Christopher -editores-Is-Law- Computable-Critical-Perspectives-on- Law-and- Artificial- Intelligence-Hart-Pu (дата звернення 05.07.2023).

464. Decentralised Identity URL: https:// www. gsma.com/ identity/ decentralised- identity (дата звернення 05.07.2023).

465. Decentralized Identity: The Ultimate Guide 2023 October 23, 2023. URL: https:// www.dock.io/post /decentralized-identity (дата звернення 05.07.2024).

466. Declaration on freedom of political debate in the media (Adopted by the Committee of Ministers on 12 February 2004. Council of Europe Committee of Ministers. URL: https://rm.coe.int/09000016805dddf8 (дата звернення 08.07.2023).

467. Declaration of Principles «Building the Information Society: A Global Challenge to the New Millennium» United Nations. World Summit on the Information Society. 2003: Geneva. URL: https:// digitallibrary.___un.org/record/ 533621/?v=pdf&ln=ru (дата звернення 05.07.2023).

468. Décision n 2009-580 DC du 10 juin 2009. Conseil constitutionnel. URL: https:// www.conseil-constitutionnel.fr/decision/2009/2009580DC.htm (дата звернення 05.07.2023).

469. Deelmann T., Loos P. Trust economy: aspects of reputation and trust building for SMEs in E-business. URL: http://aisel.aisnet.org/amcis2002/302 (дата звернення 07.07.2023).

470. Delacroix S., Lawrence N. Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance. *International Data Privacy Law*. October 12, 2018. P. 1-43. URL: https:// ssrn.com/ abstract=3265315 (дата звернення 06.07.2023).

471. Dellarocas C. The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms. *Special Issue on E-Business and Management Science.* 2003. № 10. P. 1407-142. URL: https:// www.jstor.org/ stable/4134013# (дата звернення 06.07.2023).

472. Deleuze G., Guattari F. L'Anti-Oedipe. Capitalisme et schizophrénie Publicado en francés por Les Éditions de Minuit, París, 1972. 493 p.

473. Deleuze G. The logic of Sense. Columbia University Press. Edited by Constantin V. Boundas. Translated by Lester M. & Stivale C. 1990. 393p.

474. Denby K. Bloggers Who Risked All to Reveal the Junta's Brutal Crackdown in Burma. Times Online, Oct. 1, 2007. URL: http:// www.timesonline.co. uk/tol/news/ world/asia/article2563937.ece (дата звернення 05.07.2023).

475. Derham D. Theories of legal Personality. *Legal Personality and Political Pluralism.* in Leicester C. Webb (ed.). Melbourne University Press.1958. P. 1-19.

476. Did the Internet Kill Privacy? CBS News. February 6, 2011. URL: https://www.cbsnews.com/news/did-the-internet-kill-privacy/ (дата звернення 05.07.2023).

477. Digital Rights Litigation Guide. Media Legal Defence Initiative. 2020. URL: https:// www. mediadefence. org/ wp-content/uploads/ 2020/06/MLDI-Training- Manual-on- Digital -Rights-and-Freedom - of-Expression-Online.pdf. P. 5. (дата звернення 08.08.2023).

478. Digital solutions for pharma & life sciences. URL: https:// www.avenga.com/industries/pharma-life-sciences/ (дата звернення 08.08.2023).

479. Digital Twin Use Cases and Applications URL: https://softengi.com/blog/use-cases-and-applications-of-digital-twin/ (дата звернення 10.10.2023).

480. Digital Twins URL: https://www.it.ua/knowledge-base/technology-innovation/cifrovoj-dvojnik-digital-twin (дата звернення 08.10.2023).

481. Different types of internet cookies URL: https:// www.rocketlawyer. com/gb/en/ business/run-an-online-business/ legal-guide/different-types-of-internet-cookies (дата звернення 09.10.2023).

482. Drexl J., Hilty R., Desaunettes L. Data Ownership and Access to Data. URL: http://www.ip.mpg.de/en/link/positionpaper-data-2016-08-16.html (дата звернення 08.08.2023).

483. Drexl J., Hilty R., Globocnik J. Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's "Public consultation on Building the European Data Economy". URL: www.ip. mpg.de/fileadmin/ipmpg/content/ stellungnahmen/MPI_

Statement_Public_consultation_on_ Building_the_ EU_Data_Eco _28042017.pdf (дата звернення 08.09.2023).

484. Dressel J., Farid H. The Dangers of Risk Prediction in the Criminal Justice System. MIT Schwarzman College of Computing. 2021. URL: https:// mit-serc. pubpub. org/pub/risk-prediction-in-cj/release/2 (дата звернення 09.08.2023).

485. Dressel J., Farid H. The accuracy, fairness, and limits of predicting recidivism. *Science Advances*. 2018. №4 (1). URL: doi:10.1126/sciadv.aao5580 (дата звернення 09.08.2023).

486. Donath J.S. Identity and deception in the virtual community. *Communities in cyberspace*. 1996. p. 29-59. URL: http://onlinelibrary. wiley. com/doi /10.1002/asi. 23552/abstract (дата звернення 08.10.2023).

487. Duclercq J.-B. L'automatisation algoritmique des décisions administratives individuelles. *Revue du droit public.* 2019. № 2. P. 295-320.

488. Duranske B. Virtual law: navigating the legal landscape of virtual worlds. American Bar Association Publisher. 2008. 250 p.

489. Easterbrook F.H. Cyberspace and the Law of the Horse. *University of Chicago Legal Forum*. 1996. № 1. P. 207-216. URL: https://chicagounbound.uchicago.edu/uclf/vol1996/iss1/7 (дата звернення 13.08.2023).

490. E-Government Survey 2020. Digital Government in the Decade of Action for Sustainable Development. With addendum on COVID-19 Response. Department of Economic and Social Affairs. UNITED NATIONS New York, 2020. 323p. URL: https://publicadmin istration.un.org/egovkb/ Portals/egovkb/ Documents/un/ 2020-Survey/ 2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf (дата звернення 12.10.2023).

491. EGovernment Benchmark 2024. Insight Report. European Commisson URL: https://www.capgemini.com/wp-content/uploads/2024/07/eGovernment-Report-2024.pdf (дата звернення 08.12.2024).

492. European Data Protection Law and Practice Second Edition Executive Editor Eduardo Ustaran, Second edition. IAPP. CIPP/E Partner, Hogan Lovells. Hyde Park Publishing Services. 2019. 281 p.

493. European Parliament. Report with recommendations to the Commission on Civil Law Rules on Robotics 2015/2103 INL. 27.01.2017. URL: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html (дата звернення 06.09.2023).

494. European protection in good health? / ed. by S. Gutwirth, R. Leenes, P. De Hert, Y. Poullet. Springer Science & Business Media, 2012. 363p.

495. European Strategy for Data 19.02.2020 European Comission 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066

496. Edunov S., Bhagat S. et al., Three and a Half Degrees of Separation, Facebook research. February 4, 2016. URL: https://research.fb.com/blog/2016/02/three-and-a-half-degrees-of-separation/___(дата звернення 05.05.2023).

497. Eidenmueller H. The Rise of Robots and the Law of Humans. *Oxford Legal Studies Research Paper*. 2017. № 27. P. 1-15. URL: http://ssrn.com/abstract=2941001 (дата звернення 05.08.2023).

498. Eisenlauer V. Facebook: A multimodal discourse analysis of (semi-) automated communicative modes. Interactions, Images and Texts: A Reader of Multimodality / ed. by C. Maier, S. Norris. Berlin: de Gruyter, 2014. P. 311-322. DOI:10.1515/9781614511175.311

499. Elamroussi A. This Washington county is the first to ban facial recognition technology, official says. URL: https:// edition.cnn.com /2021/06/02/us/ facial-recognition -technology-ban/index.html (дата звернення 05.05.2023).

500. Electronic Communications Privacy Act of 1986. USC 2510. URL: https://www.loc.gov/law/opportunities/ PDFs/ ElectronicCommunications PrivacyAct- PL199-508.pdf (дата звернення 05.05.2023)/

501. Evans-Pughe C. Will robots steal our jobs? *Engineering & Technology*. 2017. № 9. URL: https://doi.org/10.1049/et.2017.090 (дата звернення 05.05.2023).

502. Equal Credit Opportunity Act. 1974 URL: https:// www. govinfo.gov/ content /pkg/ USCODE-2011 -title15/ html/USCODE -2011-title15-chap41-subchapIV.htm (дата звернення 05.05.2023).

503. Equality Act. UK Public General Acts. 8th April 2010. URL: https://www.legislation.gov.uk/ukpga/2010/15/contents (дата звернення 05.05.2024).

504. Erdös P., Rényi A. On the Evolution of Random Graphs. *Publication of the Mathematical Institute of the Hungarian Academy of Sciences.* 1960. № 5. P. 17-61. URL: https://snap.stanford.edu/class/cs224w-readings/erdos60random.pdf(дата звернення 03.04.2024).

505. Eszter H. The Digital Divide and what to do about it. San Diego: Academic Press, 2003. URL: http://www.eszter.com/research/pubs/hargittai-digitaldivide.pdf (дата звернення 05.04.2023).

506. Ethical design and use of automated decision systems. *The Standards Council of Canada*. 2019. URL: https://www.scc.ca/en/standardsdb/standards/29998 (дата звернення 09.05.2023).

507. Evans-Pughe C. Our Surveillance Society Goes Online, Guardian. May 8, 2008. URL: https://www.theguardian.com/technology/2008/may/08/privacy.internet (дата звернення 03.03.2024).

508. Facial recognition regulation in the USA: an efficient legal patchwork? *Mathias Avocats*. 2020. URL: https://www.avocats-mathias.com/donnees-personnelles/facial-recognition-usa (дата звернення 05.12.2022).

509. Fair Housing Act 1968 (Title VIII of the Civil Rights Act) URL: https://www.justice.gov/crt/fair-housing-act-2(дата звернення 03.03.2023).

510. Farid H. The danger of predictive algorithms in criminal justice. TEDxAmoskeagMillyard. URL: https://m.youtube.com/watch?v=p-82YeUPQh0&pp=ygUVcHJlZGljdGllZCBhaSBqdXN0aWNl___(дата звернення 03.05.2024).

511. Fazlioglu M. Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet. *International Data Privacy Law*. 2013. № 3. P. 149-157.

512. Federal Act on Human Genetic Testing (HGTA) 8 October 2004. The Federal Assembly of the Swiss Confederation. URL: https://www.fedlex.admin.ch/eli/cc/2007/131/en (дата звернення 03.03.2023).

513. Federal German Data Protection Act (Bundesdatenschutzgesetz, BDSG) URL: https://germanlawarchive.iuscomp.org/?p=712(дата звернення 14.12.2022).

514. Fetscherin M. CD Present State and Emerging Scenarios of Digital Rights Management Systems. *The International Journal on Media Management.* 2002. № 3. Vol. 4. P. 164-171.

515. Flak L., Hofmann S. The Impact of Smart City Initiatives on Human Rights. August 21, 2020. URL: https://ceur-ws.org/Vol-2797/paper16.pdf (дата звернення 05.12.2022).

516. Finck M., Pallas F. They who must not be identified – distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law.* 2020. № 1(10). P. 11.

517. Fischer J.P. Computers as Agents: A Proposed Approach to Revised U.C.C. Article 2. *Indiana. Law Journal.* 1997. № 2 (72). P. 538-573.

518. Flückiger A. L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété? *Pratique juridique actuelle.* 2013. № 6. Vol. 22. P. 837-864.

519. Floridi L. The Right to Be Forgotten: a Philosophical View. *Annual Review of Law and Ethics.* 2015. P. 1-16. URL: https://www. academia.edu/16491066/_The_Right_ to_Be_Forgotten_ a_Philosophical_ View_forthcoming _in_Annual_Review_of_Law_and_Ethics (дата звернення 05.12.2022).

520. Floridi L. The Informational Nature of Personal Identity. 2011. May 5. P. 1-18. URL: https://ssrn.com/abstract=3840132 (дата звернення 08.12.2023).

521. Fialova E. Data Portability and Informational Self-Determination. *Masaryk University Journal of Law and Technology*. 2014. № 1 (8). P. 45-55. URL: https:// journals.muni.cz /mujlt/article/view/2645(дата звернення 05.04.2023).

522. Filippi P.D., Hassan S. Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*. 2016. № 21(12). URL: https://doi.org/10.5210/fm.v21i12.7113_(дата звернення 07.05.2023).

523. Fourcade M., Healy K. Classification situations: Life-chances in the neoliberal era. *Historical Social Research.* 2007. №. 1 (159). Vol. 42. P. 23-51. URL: https://www.jstor.org/stable/44176023 (дата звернення 05.09.2022).

524. Freedom of Expression on the Internet. OSCE Representataive on Freedom of the Media. 15 December 2011. URL: https://www.osce.org/fom/80723 (дата звернення 05.12.2022).

525. Frosini T.E. The Internet Access as a Fundamental Right. *Studies in Law: Research Materials*. 2014. № 1. P. 5-12.

526. Fuchs A. What happens to your social media account when you die? The first German judgments on digital legacy. *ERA Forum*. 2021. № 22. P.1-7. URL: https://doi.org/10.1007/s12027-021-00652-y (дата звернення 05.08.2022).

527. Fussell S. The Next Target for a Facial Recognition Ban? 28.01.2021. New York URL: https://www.wired.com/story/next-target-facial-recognition-ban-new-york/ (дата звернення 08.06.2022).

528. Gacutan J., Selvadurai N. A statutory right to explanation for decisions generated using artificial intelligence. *International Journal of Law and Information Technology*. 2020. № 3. Vol. 28. P. 193-216.

529. Gander M. Managing your personal brand. *Perspectives: Policy and Practice in Higher Education*. 2014. № 3. P. 99-102. URL: DOI:10.1080/13603108.2014.913538

530. GenBank Overview. National Genetic Database. URL: https://www.ncbi.nlm.nih.gov/genbank/ (дата звернення 05.12.2022).

531. Georges F., Seilles A., Artignan G., Arnaud B., Rodriguez N. Sémiotique et visualisation de l'identité numérique: une étude comparée de Facebook et Myspace. 2009. URL: https://hal-lirmm.ccsd.cnrs.fr/hal-00410952/document (дата звернення 05.10.2022).

532. Getting Married in the Metaverse. June 22, 2023. URL: https://www. nytimes.com /2021/12/08/ fashion/metaverse-virtual-wedding.html(дата звернення 18.12.2023).

533. Gendiagnostikgesetz vom 31. Juli 2009 (BGBl. I S. 2529, 3672), das zuletzt durch Artikel 15 Absatz 4 des Gesetzes vom 4. Mai 2021. (BGBl. I S. 882) geändert worden ist. URL: https://www. gesetze-im-internet.de/gendg/index.html#BJNR252900009BJNE001000000 (дата звернення 05.11.2023).

534. Gershgorn D. Maine passes the strongest state facial recognition ban yet. June 30, 2021. URL: http://https// www.politico.eu/ article/european- parliament-ban-facial- recognition-brussels/ (дата звернення 05.12.2022).

535. Gillis T.B., Spiess J.L. Big Data and Discrimination. *University of Chicago Law Review*. 2019. № 2. Vol. 86. P. 459-487. URL: https://chicagounbound. uchicago. edu/uclrev/ vol86/iss2/4 (дата звернення 05.12.2022).

536. Gillis T. Talks about her recent paper “Big Data and Discrimination” (Harvard University) URL: https://www. youtube. com/watch?v=fhv-rqRkobg (дата звернення 05.10.2022).

537. Giordano F. Invoking Law as a Basis for Identity in Cyberspace. *Stanford Technology Law Review*. 1998. № 1. P. 1-79.

538. Goldman E. The Privacy Hoax. URL: https:// www. forbes.com /forbes/2002/ 1014/042.html?sh=7734abb02717 (дата звернення 08.06.2022).

539. Goddard K., Roudsari A., Wyatt J. Automation bias: a systematic review of frequency, effect mediators, and mitigators. *Journal of the American Medical Informatics Association*. 2012. № 1. P. 121-127. URL: https://doi.org/10.1136/amiajnl-2011-000089 (дата звернення 05.12.2023).

540. Goggin G., Vromen A., Weatherall K. Digital Rights in Australia. *Sydney Law School Research Paper*. 2017. № 18-23. URL: https://ssrn.com/abstract=3090774 (дата звернення 11.11.2023).

541. Goodman B., Flaxman S. EU Regulations on Algorithmic Decision Making and “a Right to an Explanation”. June 28, 2016. URL: https:// ora.ox.ac.uk

/objects/ uuid: 593169 ee-0457 -4051-9337-e007064cf67c/ download_file? safe_filename=euregs.pdf&file_format=application%2Fpdf&type_of_work=Journal+ article [https://perma.cc/C6UP-DZQE(дата звернення 05.12.2022).

542. Google yourself. What do you see? Are you represented fairly? URL: https://uk. reputationdefender. com/what-online- reputation-management (дата звернення 05.05.2023).

543. Granovetter M.S. The Strength of Weak Ties. *American Journal of Sociology*. 1973. № 6. Vol. 78. P. 1360-1380. URL: https://www. jstor.org/stable / 2776392? read-now=1&seq=5 (дата звернення 05.12.2022).

544. Grochowski M. Inheritance of the Social Media Accounts in Poland. *European Review of Private Law.* 2019. №. 5. P. 1195-1206. URL: https://ssrn.com/abstract=3470427 (дата звернення 12.12.2022).

545. Grohol J. Anonymity and Online Community: Identity Matters. 2006. № 214. URL: https://alistapart.com/article/identitymatters/(дата звернення 05.11.2022).

546. Guadamuz A. Costa Rican court declares the Internet as a fundamental right October 2, 2010. URL: https://www.technollama.co.uk/costa-rican-court-declares-the-internet-as-a-fundamental-right (дата звернення 05.11.2022).

547. Guernsey L. Welcome to the World Wide Web. Passport, Please? *The New York Times*. March 15, 2001. URL: http://www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html (дата звернення 05.12.2022).

548. Hamari J., Sjöklint M., Ukkonen A. The sharing economy: why people participate in collaborative consumption. *Journal of the association for information science and technology.* 2016. Vol. 67 (9). P. 2047-2059.

549. Hassler S. Do We Have to Build Robots That Need Rights? North American. 06 March 2017. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp? ar-number=7864739. (дата звернення 05.05.2023).

550. Hassan S., De Filippi P. The Expansion of Algorithmic Governance: From Code is Law to Law is Code. *Field Actions Science Reports*. 2017. № 17. P. 88-90. URL: http://journals.openedition.org/factsreports/4518 (дата звернення 09.05.2023).

551. Halperin R., Backhouse J. A roadmap for research on identity in the information society. *Identity in the Information Society*. 2008. Vol. 1 (1). P. 71-87. URL: https://link.springer.com/article/10.1007/s12394-008-0004-0 (дата звернення 09.05.2023).

552. Hauben M. The Net and Netizens: The Impact the Net has on People's Lives. Netizens: an anthology. 2008. P. 141. URL: http://www.columbia.edu/~hauben/(дата звернення 08.03.2024).

553. Herbert S. Digital Memoralization: Collective Memory, Tragedy, and Participatory Spaces. A thesis presented to the Faculty of Arts and Humanities. Denver, 2008. 125 p.

554. Hert P., Papakonstantinou V., Malgieri G., Beslay L. The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services. *Computer Law and Security Review.* 2018. № 2. P. 193-203. URL: https://ssrn.com/abstract=3447060 (дата звернення 24.09.2024).

555. Herrschaft B.A. Evaluating the reliability and validity of the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) 2014. URL: https://rucore.libraries.rutgers.edu/rutgers-lib/46260/#citation-export (дата звернення 24.09.2024).

556. Hesselberth P. Discourses on dysconnectivity and the right to disconnect, *New Media & Society*. 2018. № 20 (5). P. 1994-2010. URL: https://core.ac.uk/download/pdf/269294823.pdf (дата звернення 26.11.2024).

557. Hildebrandt M. Criminal Law and Technology in a Data-Driven Society. *Dubber M. D., Hörnle T.* (eds.). The Oxford Handbook of Criminal Law. Oxford, 2014. P. 174-200.

558. Hildebrandt M. Profiling and the rule of law. Identity in the Information Society. 2008. Vol. 1. P. 55-70. URL: DOI: 10.1007/s12394-008-0003-1.

559. Hill K. Google's Eric Schmidt Says Plus Is An 'Identity Service' Not A Social Network. August 29, 2011. URL: https://www.forbes.com/sites/kashmirhill/2011/08/29/googles-eric-schmidt-says-plus-is-an-identity-service-not-a-social-network/(дата звернення 08.03.2024).

560. Hintze M. In defense of the long privacy statement (The state of cyberlaw: Security and privacy in the digital age). *Maryland Law Review.* 2017. № 76. P. 1044-1085. URL: https://ssrn.com/abstract=2910583 (дата звернення 08.03.2024).

561. Hodgson V. Issues for Democracy and Social Identity in CMC and Networked Learning.Chapter. Networked Learning: Perspectives and Issues, (eds) Steeples C. Jones C. Springer Verlag, London 2002. P. 229-242. URL: https://link.springer.com/chapter/10.1007/978-1-4471-0181-9_13 (дата звернення 05.10.2024).

562. Holton R.J. Global Networks. Red Globe Press. 2007. 224 p.

563. Holvast J. History of Privacy. The Future of Identity in the Information Society. Privacy and Identity Chapter. *Advances in Information and Communication Technology.* 2009. Vol. 298. P. 13-42. URL: https://doi.org/10.1007/978-3-642-03315-5_2

564. Hood L., Auffray C. Participatory medicine: a driving force for revolutionizing healthcare. *Genome medicine.* 2013. № 5 (110). P. 2-4. URL: doi:10.1002/biot.201100306.

565. Hooghiemstra T. Informational Self-Determination, Digital Health and New Features of Data Protection. *European Data Protection Law Review.* 2019. №2. Vol. 5. P. 161-174. DOI: 10.21552/edpl/2019/2/6

566. How to Create a Memorial Page on Facebook and Instagram. URL: https://www. funeralbasics.org/ memorial-page- facebook-instagram/ (дата звернення 08.10.2024).

567. How do the cookie rules relate to the GDPR? Information commissioner's office UK. URL: https://ico.org.uk/ for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/ guidance-on-the-use-of-cookies-and-similar-technologies/ how-do-the-cookie-rules-relate-to-the-gdpr/#GDPR1 (дата звернення 08.10.2024).

568. How modern data protection is helping to unlock the power of data. Elizabeth Denham’s keynote speech. 2021. URL: https://www.wired-gov.net/wg/

news.nsf/articles/ How+modern+data+ protection+is +helping+ to+ unlock+the+power+of+data+13052021122500?open (дата звернення 13.06.2024).

569. How redlining prevented Black and Brown families from becoming home owners. Video. 2023. URL: https://_www.youtube. com/watch? v=cUl3l4w5CYw (дата звернення 08.03.2024).

570. Howes D. E-Legislation: Law-Making in the Digital Age. *McGill Law Journal.* 2001. Vol. 47. P. 39-57.

571. Human Rights in the Age of Platforms. edited by R.F. Jørgensen, J. Van Hoboken *The privacy disconnect*. 2019. The MIT Press. 345 p. URL: https://doi.org/10.7551/mitpress/11304.003.0017 (дата звернення 24.09.2024).

572. Human Rights Watch Submission on Draft General Recommendation No. 36 on Preventing and Combatting Racial Profiling 17 December 2020.CERD/C/GC/36 URL: https://www.ohchr.org/ en/documents/general- comments- and-recommendations/ general -recommendation- no-36-2020-preventing-and (дата звернення 21.05.2024).

573. ISO/IEC 27701:2019: Are you ready for the new privacy information management standard? March 24, 2020 URL: https://www.advantio.com/blog/iso-iec-27701-2019-are-you-ready-for-the-new-privacy-information-management-standard (дата звернення 05.04.2024).

574. ISO/IEC JTC 1/SC 37 Biometrics URL: https://www.iso.org/ru/committee/313770.html (дата звернення 24.09.2024).

575. ICRC Position Paper: Artificial intelligence and machine learning in armed conflict: A human-centred approach. March 2021. International Review of the Red Cross. URL: https://international-review.icrc.org/articles/ai-and-machine-learning-in-armed-conflict-a-human-centred-approach-913 (дата звернення 24.03.2024).

576. ICRC position on autonomous weapon systems. International Commitee of the Red Cross. May 12, 2021. URL: https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems (дата звернення 12.04.2024).

577. Identity Definition & Meaning. URL: https://www.dictionary.com/browse/identity(дата звернення 02.02.2024).

578. IMD Smart City 2023. World Competitiveness Center. URL: https://we-gov.org/news-2023/imd-samrt-city-index-2023-published-in-partnership-with-wego/?ckattempt=1(дата звернення 08.03.2024).

579. Internet Governance. Infrastructure and Institutions. Edited by Bygrave L.A., Bing J. 2009. Oxford University Press. 262 p.

580. Jameson F. Postmodernism, the Cultural Logic of Late Capitalism. 1991. P. 53-91. URL: https:// web.education. wisc.edu/ halverson/ wp-content/ uploads/ sites/33/ 2012/12/jameson.pdf (дата звернення 08.05.2023).

581. Jasmontaite L., De Hert P. Access to the Internet in the EU: A Policy Priority, a Fundamental, a Human Right or a Concern for eGovernment? *Brussels Privacy Hub Working Paper*. 2020. №. 6 (19). P. 1-24. URL: https://ssrn.com/abstract=3535718 (дата звернення 09.03.2024).

582. Jeng Y.-L. An OpenID Based Authentication Mechanism in a Distributed System Environment. *International journal of Computer and Communication Engineering*. 2012. № 3. P. 250- 252.

583. Jenkins H., Shresthova S., Gamber-Thompson L., Kligler-Vilenchik N., Zimmerman A. *By Any Media Necessary: The New Youth Activism*, New York, USA: New York University Press, 2016. P. 1482-1484. https://doi.org/10.18574/nyu/9781479829712.001.0001(дата звернення 24.09.2024).

584. Jennejohn M. The Architecture of Contract Innovation. *Boston College Law Review*. 2018. № 59 P. 71-143. URL: https://ssrn.com/abstract=3081946 (дата звернення 20.10.2024).

585. Johnson A. Aug 30, 2022, Digital Identities Will Change. The Nature of Online Reputation URL: https://www.forbes.com/sites/alastairjohnson/2022/08/30/digital-identities-will-change-the-nature-of-online-reputation/?sh=4f43673b584a (дата звернення 20.10.2024).

586. Joined cases C-92/09 and C-93/09. Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen. 2011. *CJEU / Court of Justice of The European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62009CA0092 (дата звернення 20.11.2022).

587. Joyce D. Internet Freedom and Human Rights. *European Journal of International Law*. 2015. № 26(2). P. 493-514. https://doi.org/10.1093/ejil/chv021 (дата звернення 20.10.2023).

588. Jurcys P. Personal Data Ownership 23.07.2020. URL: https://towardsdatascience.com/personal-data-ownership-f3b62e6ed07d (дата звернення 21.07.2024).

589. Jurcys P., Donewald C., Fenwick M. et al. A. Ownership of user-held data: why property law is the right approach. *Harvard Journal of Law and Technology Digest.* 2021. P. 1-30. URL: https://ssrn.com/abstract=3711017 (дата звернення 21.07.2024).

590. Kahler M., Networked politics: agency, power, and governance. Cornell University Press. 2011. URL: https://citeseerx. ist.psu.edu/document?repid =rep1&ф=pdf&doi=257 daaefc0437f691843fa90f784e4b c1c87 ecde (дата звернення 24.11.2023).

591. Kalachenkova K.O., Mikhailina T.V. The role of digital rights in the modern states stable development: problems of recognition and legalization. *Науковий вісник Ужгородського Національного Університету.* 2023. № 75. С. 91-98.

592. Karjoth G., Schunter M. Waidner M. Platform for enterprise privacy practices: privacy-enabled management of customer data. in 2nd international conference on Privacy enhancing technologies. 2002. P. 69-84. URL: http://d ud.inf.tu-dresden. de/sirene/publ/KaSW1_02.EP3P4PET.pdf (дата звернення 24.10.2023).

593. Karnow C. Liability for Distributed Artificial Intelligences. *Berkerley Technology Law Journal.* 1996. № 11. P. 161-162.

594. Karppinen K., Puukko O. Four Discourses of Digital Rights: Promises and Problems of Rights-Based Politics. *Journal of Information Policy*. 2020. № 10. P.

304-328. URL: https://www.jstor.org/stable/10.5325/jinfopoli.10.2020.0304 (дата звернення 20.10.2023).

595. Kim T.W., Routledge B.R. Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach. 2020. P. 1-43. URL: https:// ssrn. com/abstract=3716519 (дата звернення 22.10.2023).

596. Kim T.W., Routledge B.R. Algorithmic transparency, a right to explanation and trust. Squarespace. June 2017. URL: https:// static1.squarespace.com/static/5 92ee286d482e908d35b8494/t/ 5955241 5579fb30c 014cd06c/ 1498752022120/Algorithmic +transparency%2C+ a+right+to+ explanation+and+trust+ %28TWK%26BR% 29.pdf (дата звернення 23.10.2023).

597. Kirkpatrick D. The Facebook Effect: The inside Story of the Company That Is Connecting the World. New York, 2011. 384 p.

598. Kelly K. The Next 30 Digital Years. URL: https://www.youtube.com/watch?v=XhduPAy2bxo (дата звернення 21.11.2024).

599. Kettemann M. UN Human Rights Council Confirms that Human Rights Apply to the Internet. Blog of the European Journal of International Law. July 23, 2012. URL: https://www. ejiltalk.org/ un-human-rights-council-confirms- that-human-rights-apply-to-the-internet/(дата звернення 22.05.2023).

600. Kobie N. The complicated truth about China’s social credit system. URL: https://www._wired.com/story/ china-social-credit-system-explained/ (дата звернення 21.08.2023).

601. Kobryn P.A. The digital twin concept. In Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2019 Symposium. National Academy of Engineering. 2020. P. 17-24. URL: https:// doi.org/10.17226/25620 (дата звернення 05.06.2024).

602. Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security.* 2017. № 64. P. 122-134. URL: https:// www.sciencedirect.com /science/ article/abs/ pii/S0167404815001017 (дата звернення 20.07.2023).

603. Koster R. Declaring the Rights of Players, Aug. 27, 2000. URL: http://www. raphkoster.com/gaming/playerrights.shtml. (дата звернення 21.09.2024).

604. Kowalska R. Natural Person vs. Legal Person: A Comprehensive Comparison of Rights and Responsibilities. Wirtualnebiuropoznan. 2023. October 25. URL: https:// wirtualnebiuropoznan.pl /en/2023/10/25/ natural-person -vs-legal-person-a-comprehensive-comparison-of-rights-and-responsibilities/ (дата звернення 20.02.2024).

605. Kuhling J., Neumann K. Ökonomische und rechtliche Rahmenbedingungen zum Ausbau und zur Finanzierung von Breitband-Hochleistungsinfrastrukturen in dünn besiedelten Gebieten' in R. Inderst et al., *Der Ausbau neuer Netze in der Telekommunikation*, Nomos, 2012. P. 201-204.

606. Kumayama K.D. A right to pseudonymity. *Arizona Law Review.* 2009. № 51. P. 427-464.

607. Kuner C. An international legal framework for data protection: Issues and prospects. Computer Law & Security Review. 2009. Vol 25(4). P. 307-317. URL: https://ssrn.com/abstract=1443802 (дата звернення 20.07.2023).

608. Kurzweil R., Grossman T. Fantastic voyage: live long enough to live forever. The science behind radical life extension questions and answers. *Studies in Health Technology and Informatics.* 2009. № 149. P. 187-194. URL: https://pubmed.ncbi.nlm.nih.gov/19745481/(дата звернення 21.07.2022).

609. Korea Produces Safer Online Registration Guidelines URL: http://english.chosun.com/ w21data/html/news/200610/200610020023.html (дата звернення 21.07.2022).

610. Kosinski M., Stillwell D., Graepel T. Private traits and attributes are predictable from digital records of human behaviour. *Proceedings of the National Academy of Sciences.* 2013. № 15. P. 5802-5805. URL: www.pnas. org/content/early/2013/03/06/1218772110. (дата звернення 27.07.2023).

611. Hiq Labs, Inc. V. Linkedin corporation. November 04.11. 2022. № 17-16783. URL: https://caselaw.findlaw.com/court/us-dis-crt-n-d-cal/2182242.html (дата звернення 22.10.2023).

612. Laumann E.O. Comment on The Future of Bureaucracy and Hierarchy in Organizational Theory: A Report from the Field. In Bourdieu, P. and Coleman, J.S. (editors) Social Theory for a Changing Society. Boulder, CO: Westview, 1991. P. 90-93.

613. Larsen K. M. Analytics fights human trafficking using Amazon Rekognition. 09 AUG 2018 URL: https://a__ws.amazon.com/blogs/__machine-learning/marinus-analytics-fights-human- trafficking-using-amazon-rekognition/ (дата звернення 10.02.2024).

614. La Rue F. UN. Human Rights Council. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Geneva. A/HRC/23/40 UN, 17 April 2013. URL: https://digitallibrary.un.org/record/756267?ln=ru&v=pdf (дата звернення 28.07.2023).

615. La Rue F. UN Human Rights Council. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 May 2011, A/HRC/17/27 URL: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf . (дата звернення 27.07.2022).

616. Lastowka G.F., Hunter D. The Laws of the Virtual Worlds. *California Law Review.* 2004. № 1 (92). P. 1-72.

617. Latour B. On technical mediation – philosophy, sociology, genealogy. *Common Knowledge.* 1994. № 3(2). P. 29-64.

618. Latour B. Reassembling the social: An introduction to actor-network-theory. Oxford University Press, USA. 2005. 295 p.

619. Latour B. Science in action: How to follow scientists and engineers through society. Cambridge, MA: Harvard University Press. 1987. 288p.

620. Latour B. On actor-network theory: A few clarifications. *Soziale Welt*. 1996. № 4 (47). P. 369-381. URL: http://www.jstor.org/stable/40878163. (дата звернення 10.02.2024).

621. Law J. Notes on the Theory of the Actor Network: Ordering. Strategy and Heterogeneity. *Systemic Practice and Action Research*. 1992. № 5 (4). P. 379-393. http://www. lancs.ac.uk/ fass/sociology/ papers/law-notes- on-ant.pdf (дата звернення 20.05.2023).

622. Lavi M. Content Providers' Secondary Liability: A Social Network Perspective. *Fordham Intellectual Property Media & Entertainment Law Journal.* 2016. № 4. P. 855-943. URL: https://ir.lawnet.fordham .edu/iplj/vol26/ iss4/2/(дата звернення 21.07.2023).

623. Lazer D. Networks and Politics: The Case of Human Rights, *in* Understanding social action, promoting human rights. R. Goodman, D. Jinks, A.K. Woods, Oxford University Press. 2012. P. 244-264.

624. Li Y. As China's Internet Disappears, 'We Lose Parts of Our Collective Memory. June 4, 2024. URL: https:// www.nytimes.com /2024/06/04/ business/ china-internet- censorship.html (дата звернення 20.12.2024).

625. Lee J. Death and Live Feeds: Privacy Protection in Fiduciary Access to Digital Assets. *Columbia Business and Law Review.* 2015. № 2. P. 644-693. URL: https://ssrn.com/abstract=2591411 (дата звернення 20.10.2023).

626. Lenhart A., Purcell K., Smith A., Zickuhr K. Social Media & Mobile Internet Use Among Teens and Young Adults. Washington, D.C.: Pew Research Center.february 2010. P. 1-51. URL: https:// files.eric. ed.gov /fulltext /ED525056. pdf (дата звернення 21.07.2023).

627. Ley de Economía Sostenible 2. 2011, de 4 de marzo. URL: http://www.boe.es/diario_boe/txt. php?id=BOE-A-2011-4117 (дата звернення 27.10.2023).

628. Loi n 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés URL: https:// www.legifrance_.gouv.fr /loda/id/JOR FTEXT0000 00886460 (дата звернення 27.10.2023).

629. Loi n 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels (1) URL: https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000032984268#:~:text=«%

207°%20Les%20modalités%20du,la%20vie%20personnelle%20et%20familiale. (дата звернення 27.10.2023).

630. Loi n 2016-1321 du 7 octobre 2016 pour une République numérique. URL: https:// www.wipo.int /wipolex /en/legislation / details/16380 (дата звернення 27.10.2023).

631. Loi Informatique et Libertés 17 décembre 2015 URL: https://www. legifrance.gouv.f r/loda/id /JORFTEXT00000 0886460/ (дата звернення 21.07.2023).

632. Lemley M.A. How Generative AI Turns Copyright Upside Down. *Columbia Science and Technology Law Review*. 2024. № 25. P. 21-44. URL: https://ssrn.com/abstract=4517702 (дата звернення 13.08.2024).

633. Lemley M.A., Volokh E. Law, Virtual Reality, and Augmented Reality. *University of Pennsylvania Law Review*. 2018. № 5. P. 1052-1138. URL: https:// ssrn.com/ abstract=2933867 (дата звернення 21.07.2023).

634. Les propositions adoptées par le 113e Congrès des notaires de France. REF: Defrénois 28 September. 2017 № def129c3, P. 9. URL: https://www. defrenois.fr/article/defrenois/DEF129c3 (дата звернення 21.07.2023).

635. Lepage A. Libertés et droits fondamentaux à l'épreuve de l'internet. 2003. 328 p.

636. Lessig L. Code: And Other Laws of Cyberspace, Version 2.0. Basic Books, 2006. 410p.

637. Lessig L. The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*. 1999. № 113(2). P. 501-546. URL: https:// nissenbaum.tech. cornell.edu/papers/lawofthehorse.pdf (дата звернення 24.06.2023).

638. Lessons from the identity trail: anonymity, privacy and identity in a networked society / edited by I. Kerr, V. Steeves, C. Lucock. Monograph. Oxford University Press, 2009. 554 p.

639. Letter from Jordan McCollum, Gen.Counsel, Oculus, to Senator AlFranken. May13, 2016. URL: https: //www. franken.senate. gov/files/letter /160519_ Oculus RiftResponse.pdf [https://perma.cc/6J9Z-WCSB] (дата звернення 23.06.2023).

640. Lior A. Artificial Intelligence and Tort Law: Who Should be Held Liable when AI Causes Damages? URL: https://il.boell.org/en/2021/12/24/artificial-intelligence-ai-tort-law-and-network-theory-who-should-be-held-liable-when-ai (дата звернення 22.06.2023).

641. Lior A. The AI Accident Network: Artificial Intelligence Liability Meets Network Theory. *Tulane Law Review.* 2020-2021. № 5 (95). P. 1-58. URL: https:// ssrn.com /abstract =3561948 (дата звернення 22.06.2023).

642. Litman-Navarro K. We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. 2019. URL: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (дата звернення 22.06.2023).

643. London bombings of 2005. URL: https://www. btp.police.uk /police-forces/british-transport-police/areas/about-us/about-us/our-history/london-bombings-of-2005/ (дата звернення 18.07.2023).

644. Longman Dictionary of Contemporary English. 6 th ed. Pearson. 2015, 224 p.

645. Magrini A. The Role of Predictive Analytics in Sales Forecasting. November 15, 2023. URL: https://ssrn.com/abstract=5006903 (дата звернення 22.04.2024).

646. Malgieri G., Comande G. Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. *International Data Privacy Law.* 2017. № 4 (7). P. 243-265.

647. Malgieri G. Automated decision-making in the EU Member States: The right to explanation and other «suitable Safeguards in the national legislations. *Computer law & security review.* 2018. № 3. P. 1-4. URL: https://ssrn.com/abstract=3233611(дата звернення 25.12.2023).

648. Malgieri G., Kaminski M. Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations. *International Data Privacy Law.* 2021. № 2 (21). P. 125-144. URL: https://ssrn.com/abstract=3456224 (дата звернення 25.12.2023).

649. Mckenzie W.A. Hacker Manifesto. Harvard University Press Cambridge, England 2004. 208 p.

650. Madden M. Public Perceptions of Privacy and Security in the Post-Snowden Era. November 2014. URL: https:// www. pewresearch.org /internet/ 2014/11/12/ public-privacy-perceptions/(дата звернення 25.12.2023).

651. Maine Enacts Strongest Statewide Facial Recognition Regulations in the Country June 30, 2021 URL: https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country (дата звернення 25.12.2023).

652. Marsal-Llacuna M.-L. Building Universal Socio-cultural Indicators for Standardizing the Safeguarding of Citizens' Rights in Smart Cities. *An International and Interdisciplinary Journal for Quality-of-Life Measurement.* 2017. № 130 (2). P. 563-579.

653. Maydanyk R.A., Maydanyk N.I., Velykanova M.M. Liability for damage caused using artificial intelligence technologies. *Науковий юридичний журнал.* 2021. № 2. Т. 28. С. 151-159.

654. Maydanyk L.R. Artificial intelligence and sui generis right: a perspective for copyright in Ukraine? *Access to Justice in Eastern Europe.* 2021 № 3(11). P. 144–154. DOI: 10.33327/AJEE-18-4.3-n000076

655. Mathiesen K. Human Rights for the Digital Age. *Journal of Mass Media Ethics.* 2014. № 1. P. 2-18. Doi:10.1080/08900523.2014.863124.

656. Mathiesen K. The Human Right to Internet Access: A Philosophical Defense. *International Review of Information Ethics*. 2012. № 12. Vol. 18. P. 9-22. URL: DOI 10.29173/irie299.

657. Mattis P. China's adaptive approach to the information counter-revolution. *China Brief.* 2011. № 11 (10). P. 5-6. URL: https://jamestown.org/program/chinas-adaptive-approach-to-the-information-counter-revolution/ (дата звернення 22.02.2024).

658. Marron D. Consumer Credit in the United States. A Sociological Perspective from the 19th Century to the Present. *Present. New York*: *Palgrave Macmillan*. 2009. 260 p.

659. Martin K. Ethical Issues in the Big Data Industry. *MIS Quarterly Executive.* 2015. № 14 (2). P. 67-85. URL: https://ssrn.com/abstract=2598956 (дата звернення 04.04.2024).

660. Mayer-Schönberger V. Padova Y. Regime Change? Enabling Big Data through Europe's New Data Protection Regulation. *Columbia Science & Technology Law Review.* 2016. № 17(2). P. 315-335. URL: https://journals.library.columbia.edu/index.php/stlr/article/view/4007 (дата звернення 27.12.2022).

661. McCarthy L. Digital assets and intestacy. *Boston University Journal of Science and Technol Law.* 2015. № 21(2). P. 384-412. URL: https://www.bu.edu/jostl/files/2015/12/McCARTHY_NOTE_FINAL-web.pdf (дата звернення 20.05.2023).

662. McDonald A.M., Cranor L.F. The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society*. 2008. Vol. 4 (3). P. 543-568. *URL:* https://kb.osu.edu/server/api/core /bitstreams/a9510be5-b51e-526d-aea3-8e9636bc00cd/content (дата звернення 19.06.2023).

663. McGowan D. Networks and Intention in Antitrust and Intellectual Property. *Journal of Corporation Law.* 1999. № 24. P. 514-516.

664. Media Freedom on the Internet: An OSCE Guidebook. Written by Professor Yaman Akdeniz, commissioned by the Office of the OSCE Representative on Freedom of the Media. March 2016. URL: https://www.osce.org/files/f/documents/3/c/226526.pdf (дата звернення 17.06.2023).

665. Meints M., Gasson M. High-Tech ID and Emerging Technologies.The Future of Identity in the Information Society: Challenges and Opportunities. Ed. by: Rannenberg K., Royer D., Deuker A. Springer, 2009. P. 130-189.

666. Michalkiewicz-Kadziela E., Milczarek E. Legal boundaries of digital identity creation Legal boundaries of digital identity creation. *Internet Policy Review.*

2022. № 11(1). P. 1-13. URL: https://policyreview.info/articles/analysis/legal-boundaries-digital-identity-creation (дата звернення 11.11.2023).

667. Mildebrath H. Internet access as a fundamental right. Exploring aspects of connectivity. European Parliamentary Research Service. EPRS. 2021. URL: https://www. europarl.europa.eu/ RegData/etudes/S TUD/2021 / 696170/EPRS_STU (2021)696170_EN.pdf (дата звернення 23.10.2022).

668. Miller M.E., Spatz E.A. Unified view of a human digital twin. *Human-Intelligent Systems Integration.* 2022. № 4. P. 23-33. https://doi.org/10.1007/s42454-022-00041-x

669. Mills J.L. Privacy: The Lost Right. Oxford University Press. 2008. 391 p. URL: https://ssrn.com/abstract=3452886 (дата звернення 27.12.2023).

670. Moukas A., Guttman R., Zacharia G., Maes P. Agent-mediated Electronic Commerce: An MIT Media Laboratory Perspective. *International Journal of Electronic Commerce*. 2000. P. 1-28. DOI: 10.1080/10864415.2000.11518369

671. Michael G.H.A. Game Theory Approach to Measuring the Performance Reliability of Transport Networks. Transportation research part b: methodological. 2000. № 6 (34). P. 533-545. DOI:10.1016/S0191-2615(99)00042-9

672. Mikk T., Sein K. Digital Inheritance: Heirs' Right to Claim Access to Online Accounts under Estonian Law. *Juridica International.* 2018. № 27. P. 117-128. URL: https://www.researchgate.net /publication/328658520_ Digital_Inheritance_Heirs%27_ Right_to_Claim_ Access_to_Online_ Accounts_under_ Estonian_Law (дата звернення 20.07.2023).

673. Mensel R.E. Kodakers Lying in Wait, Amateur Photography and the Right of Privacy in New York. *American Quarterly*. 1915 (1991). № 42. P. 24-45. URL: https://web. mit.edu /uricchio /Public/Documents/ media-in-transition/ Mensel-Kodakers% 20Lying%20In%20Wait.pdf (дата звернення 25.12.2022).

674. Merzeau L. La présence plutôt que l'identité. Documentaliste. *Sciences de l'Information.* 2010. № 1 (47). P. 32-33.

675. Morteza V.N. Person and Personality in Cyber Space: A legal analysis of virtual identity. *Masaryk University Journal of Law and Technology*. 2016. № 10 (1). P. 1-17. URL: DOI 10.5817/MUJLT2016-1-1

676. Mossberger K., Tolbert C.J., Mcneal R.. *Digital Citizenship: The Internet, Society, and Participation.* 2007.Cambridge: Mit Press. 240 p.

677. Natural person. April 2017. URL: https://legaldictionary.net/natural-person/(дата звернення 07.11.2023).

678. Natural Person. URL: https:// managementmania.com /en/natural-person (дата звернення 07.11.2023).

679. Natural person. Institut national de la statistique et des études économiques. 13/10/2016. URL: https:// www. insee.fr/en/metadonnees /definition/c1558(дата звернення 07.12.2023).

680. Definition of «natural person». URL: https://dictionary.justia.com/natural-person(дата звернення 13.12.2023).

681. Natural Person URL: https://www.lsd.law/define/natural-person (дата звернення 13.12.2023).

682. Wells Fargo online banking service hits. 15 May 2010. URL: https://www. finextra.com/ newsarticle/21398/ wells-fargo- online-banking-service-hits-15 (дата звернення 07.11.2023).

683. Network Neutrality. An Internet Society Public Policy Briefing. URL: https://www.internetsociety.org/wp-content/uploads/2021/01/ISOC-PolicyBrief-NetworkNeutrality-20151030.pdf (дата звернення 07.11.2023).

684. Network Readiness Index 2022 Ukraine URL: https://networkreadinessindex.org/country/ukraine(дата звернення 07.11.2023).

685. New cases on the right to access (Article 15 GDPR) URL: https:// www.bestdpo.net/ post/new-cases- on-the-right- to-access- article -15-gdpr (дата звернення 07.11.2023).

686. Newman L. The Privacy Battle to Save Google From Itself. November 1, 2018. URL: https://www.wired.com/story/google-privacy-data/(дата звернення 18.06.2023).

687. Newman M., Albert-László B., Duncan J. The structure and dynamics of networks. Princeton Studies in Complexity. 2006. 592 p.

688. Newman A., Zaring D.T. Regulatory Networks: Power, Legitimacy, and Compliance. *Interdisciplinary perspectives on international law and international relations: the state of the art*. J. Dunoff M. Pollack eds., Cambridge University Press, 2013. P. 244-265. URL: https:// papers.ssrn. com/sol3/ papers.cfm? abstract_id= 2293580 (дата звернення 18.06.2023).

689. Nekit K., Tokareva V., Zubar V. Artificial intelligence as a potential subject of property and intellectual property relations. *Ius Humani. Law Journal.* 2020. № 9 (1). P. 231-250. https://doi.org/https://doi.org/10.31207/ih.v9i1.227

690. Nekit K. Fiduciary management of a social media account. *Trusts & Trustees.* 2020. № 4(26). P. 295-302.

691. Mann M., Molnar A., Warren I. State of Digital Rights. 2018. 62p. URL: https://eprints. qut.edu.au/215445/1/State-of-Digital-Rights-Web.pdf (дата звернення 20.08.2023).

692. Nyssanbekova L.B., Mashimbaeva G.A., Sairambaeva Z.T., Altayeva K.Z., Rahmetova M.A. Analysis of the Concept of "Natural Person" in Public Law and Private Law Relations. Mediterranean Journal of Social Sciences. 2015. № 5 Vol 6. P. 83-87. URL: https:// www.richtmann.org /journal/index.php/ mjss/article/view/7464 (дата звернення 15.12.2023).

693. O'Connor S.M. Biometrics and Identification after 9/11. *Bender's Immigration Bulletin.* 2002. № 7. P. 1-23.URL: https://ssrn.com/abstract=299950 (дата звернення 08.12.2023).

694. OGH Österreich 24.03.2023 № 6Ob242/22i URL: https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20230324_OGH0002_0060OB00242_22I0000_000/JJT_20230324_OGH0002_0060OB00242_22I0000_000.html (дата звернення 20.12.2023).

695. Odello M. and S. Cavandoli (eds.) Emerging areas of human rights in the 21st century: The role of the universal declaration of human rights. Routledge. 2011. 192 p.

696. OECD Forum on Tax Administration. URL: https:// www_.oecd. org/en/ publications/ oecd- forum-on-tax-administration _c34863fa-en.html (дата звернення 17.05.2023).

697. Okinawa Charter on Global Information Societ. 22.07.2000. URL: https://archive.unescwa.org/okinawa-charter-global-information-society (дата звернення 07.11.2023).

698. O'Neil C. Weapons of math destruction: How big data increases inequality and threatens democracy. *Berkeley journal of employment & labor law.* 2016. Vol. 39. № 1. P. 285-292.

699. Ong E. Online Repression and Self-Censorship: Evidence from Southeast Asia. *Government and Opposition.* 2021. № 56(1). p. 141-162. doi:10.1017/gov.2019.18

700. On the protection on natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 45/46/EC (General Data Protection Regulation). Regulation EU 2016/679. The European Parliament and of the Council of 27 April 2016 European Parliament and Council of Europe. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679(дата звернення 23.12.2023).

701. On artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters 2020/2016 European Parliament resolution of 6 October 2021 6 October 2021UR: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html (дата звернення 23.12.2023).

702. On Automated Decision-Making. Directive *Government of Canada*. 2021. URL: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592 (дата звернення 18.06.2023).

703. On Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 Guidelines. 3 October 2017. WP 251 rev. 01. URL: https:// ec. europa.eu/ newsroom/ article29 /items/612053/en (дата звернення 18.06.2023).

704. On Data Protection Officers (DPOs) Guidelines 2017. wp243rev.01_en URL: https:// ec.europa.eu/ newsroom/ article29/items/ 612048 (дата звернення 18.06.2023).

705. On Examples regarding Personal Data Breach Notification. Adopted on 14 December 2021 Versio2.0. Guidelines 01/2021 European Data Protection Board. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en (дата звернення 22.06.2023).

706. On Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission (2015/2103 (INL). URL: https://www.europarl.europa.eu/doceo/ document/TA-8-2017-0051_EN.html (дата звернення 24.12.2022).

707. On consent under Regulation 2016/679 Article 29. Guidelines. Working Party 10.10.2018. WP 259 rev.01. URL: https://ec.europa.eu/newsroom/article29/items/623051/en (дата звернення 22.07.2023).

708. On the concept of personal data. Working Party 29 Opinion 4/2007. An independent European advisory body on data protection and privacy. 20 June, 2007. URL: http://ec. europa.eu/justice _ home/fsj/ privacy/index_en.htm (дата звернення 18.06.2023).

709. On transparency under Regulation 2016/679, Working Party, Guidelines. WP260 rev.01. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en (дата звернення 18.06.2023).

710. On the adequacy of the protection provided by the EU-U.S. Privacy Shield. Commission Implementing Decision (EU) 2016/1250. 12 July 2016. The European Parliament and of the Council. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG (дата звернення 18.06.2023).

711. On the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of

Commerce. 2000/520/EC: Commission Decision of 26 July 2000. URL: https://eur-lex.europa.eu/ legal-content/en /TXT/?uri= CELEX%3A 32000 D05 20 (дата звернення 18.06.2023).

712. On the Ethics of Artificial Intelligence: Recommendation UNESCO. 2021. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455 (дата звернення 20.10.2023).

713. On the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Opinion 06/2014. URL: https:// ec.europa.eu /justice/article-29/ documentation/opinion-recommendation/ files/2014/ wp217 _en.pdf (дата звернення 22.11.2023).

714. On the processing of personal data through video devices. Guidelines 3/2019. 29 January, 2020. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (дата звернення 20.07.2024).

715. On the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects Guidelines. 2/2019. URL: https:// www.edpb.europa.eu /sites/default/ files/files/file1/ edpb_guidelines-art _6-1-b-adopted_after_public_consultation_en.pdf (дата звернення 20.10.2023).

716. On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing council framework decision. Directive (EU) 2016/680. The European Parliament and The Council. 27 April 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 (дата звернення 18.10.2023).

717. On the Proposal for a regulation of the European Parliament and of the Council on European data governance EDPB-EDPS Joint Opinion 03/2021 Data Governance Act. URL: https://edps.europa.eu/data-protection/our-work/publications/opinions/joint-opinion-edps-edps-proposal-regulation-european_en (дата звернення 19.10.2023).

718. On the Protection of Privacy and Transborder Flows of Personal Data. Organisation for Economic Co-operation and Development. OECD Guidelines. 23.09.1980. URL: www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (дата звернення 25.10.2023).

719. On the right to data portability. Guidelines. 27 October, 2017. URL: https://ec.europa.eu/newsroom/article29/items/611233 (дата звернення 16.10.2023).

720. On the Regulation on a framework for the free flow of non-personal data in the European Union Guidance. COM/2019/250. 29.05.2019. URL: https://digital-strategy.ec.europa.eu/en/library/guidance-regulation-framework-free-flow-non-personal-data-european-union (дата звернення 22.11.2023).

721. On the use of analysis of deoxyribonucleic acid (dna) within the framework of the criminal justice system. Recommendation № r(92)1 of The Committee of Ministers to Member States.10.02.1992. URL: https://rm.coe.int/09000016804e54f7 (дата звернення 22.11.2023).

722. On the Use of Electronic Communications in International Contracts, United Nations Convention. New York. 18.10.2005. URL: https://digitallibrary.un.org/record/558877?ln=ru&v=pdf (дата звернення 26.10.2024).

723. OpenID Foundation. URL: http://openid.net/wg/about/(дата звернення 25.10.2023).

724. Opinion of the Court (Grand Chamber) 26 July 2017 URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=558533 (дата звернення 12.11.2023).

725. Opinion of Advocate General Pikamäe delivered on 16 March 2023.Case C-634/21. OQ v Land Hesse, Joined party: SCHUFA Holding AG. URL: https:// curia.europa.eu /juris/document/ document.jsf? text=&docid=271343 &pageIndex= 0&doclang= en&mode= lst&dir=&occ= first&part=1&cid=8514846 (дата звернення 27.06.2024).

726. Opinion of Advocate General Jääskinen delivered on 25 June 2013. Case C 131/12. Google Spain SLGoogle Inc. v Agencia Española de Protección de datos (AEPd) Mario Costeja González. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CC0131 (дата звернення 25.10.2023).

727. Opinion of advocate general Yves Bot delivered on 23 september 2015. Case c-362/14 Maximillian Schrems v Data Protection Commissioner URL: https:// curia.europa.eu /juris/document /document.jsf? docid=168421 &docl ang=en (дата звернення 17.10.2023).

728. Orgad I. the Future of Citizenship: Global and Digital. *Debating Transformations of National Citizenship* (ed. by R. Baubock). 2018. Springer. P. 353-358.

729. Overmars M. A multi-agent system framework for agent coordination and communication enabling algorithmic trading: Theses. 2012. 255p. URL:https://hdl.handle.net/10210/5100 (дата звернення 12.11.2023).

730. Oath Holdings v. Ajemian: Who Can Access Your Email Post-Mortem?10.05.2018. URL: https://jolt.law.harvard.edu/digest/oath-holdings-v-ajemian-who-can-access-your-email-post-mortem (дата звернення 20.12.2023).

731. Oxford Dictionary of Law. sixth edition. 2006. Oxford University Press. 581p.

732. Panebianco M. d'A. Digital identity: between human rights and cybercrimes. *Rivista Giuridica AmbienteDiritto.* 2021. №1. P. 1-25. URL: https:// www.researchgate.net /profile/ Manlio-Dagostino-Panebianco /publication/ 350459292_ DIGITAL_IDENTITY_ BETWEEN_HUMAN _RIGHTS_ AND_ CYBERCRIMES /links/ 617a5c25 eef53e51e1f73cc8/ DIGITAL-IDENTITY-BETWEEN- HUMAN-RIGHTS -AND- CYBERCRIMES .pdf (дата звернення 29.10.2023).

733. Paul P.K., Aithal P.S. Digital Society: It's Foundation and Towards an Interdisciplinary Field. *Advances in Information Technology, Management, Social Sciences and Education*. 2018. *December*. № 22. P. 1-6. URL: https://ssrn.com/abstract=3397902 (дата звернення 21.10.2024).

734. Parviainen J., Coeckelbergh M. The political choreography of the Sophia robot: beyond robot rights and citizenship to political performances for the social robotics market. *AI & Society*. 2020. № 36. P. 715-724. DOI: 10.1007/s00146-020-01104-w.

735. Peacock A. Human Rights and Digital Divide. Routledge. 2019. P. 108-161. URL: https://doi.org/10.4324/9781351046794

736. Peguera M. In the aftermath of Google Spain: how the 'right to be forgotten' is being shaped in Spain by courts and the data Protection Authority. *International Journal of Law and Information Technology*. 2015. Vol. 23(4). P. 325-347. (дата звернення 28.11.2023).

737. Periodic Reporting for period 2 – iBorderCtrl (Intelligent Portable Border Control System. Horizon 2020. URL: https://cordis.europa.eu/project/id/700626/reporting (дата звернення 27.12.2023).

738. Pesenti J. Intelligence An Update On Our Use of Face Recognition. November 2, 2021. URL: https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/ (дата звернення 27.12.2022).

739. Personal Information Protection Law of the People's Republic of China. 2021. URL: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021 (дата звернення 20.10.2023).

740. Penney J.W. Internet Access Rights: A Brief History and Intellectual Origins. *William Mitchell Law Review*. 2011. № 1 (38). P. 10-42. URL: https:// papers.ssrn.com /sol3/ papers.cfm? abstract_id=2029087 (дата звернення 27.12.2023).

741. Philip N. Johnson-Laird. The Computer and the Mind*:* An Introduction to Cognitive Science. Harvard University Press, 1988. P. 353-368.

742. Podolny J. M., Karen L. Page, Network Forms of Organization. *Aannual Review of Sociology*. 1998. № 24. P. 57-76.

743. Pollicino O., De Gregorio G. Privacy or Transparency? A New Balancing of Interests for the "Right to be Forgotten" of Personal Data Published in Public

Registers. *The Italian Law Journal.* 2017. № 2(3). P. 647-668. URL: https://ssrn.com/abstract=3194726 (дата звернення 28.11.2023).

744. Pollicino O. The Right to Internet Access: Quid Iuris? *A. von Arnauld The Cambridge Handbook of New Human Rights*, Cambridge University Press, January 2020. URL: https://ssrn.com/abstract=3397340 (дата звернення 07.10.2023).

745. Prince C. Do Consumers Want to Control their Personal Data? Empirical Evidence. *International Journal of Human- Computer Studies.* 2018. № 110. P. 21-32.

746. Privacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. URL: //www.epic.org (дата звернення 20.01.2024).

747. Privacy Policy Twitter URL: https://x.com/en/privacy/previous/version_16 (дата звернення 09.08.2024).

748. Privacy Policy Reddit July 31, 2023. URL: https://www.reddit.com/policies/privacy-policy (дата звернення 20.01.2024).

749. Professional account policy. General guidelines and policies. XHelp Center. URL: https://help.x.com/en/rules-and-policies/professional-account-policy (дата звернення 28.11.2024).

750. Professor wrongly labelled as racist in Charlottesville 15 August 2017. URL: https://www.bbc.com/news/world-us-canada-40935419 (дата звернення 15.10.2023).

751. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the rights to development UN General Assembly Human rights Council. written statement / submitted by the Commonwealth Human Rights Initiative. A/HRC/32/1 27 June 2016. URL: https://digitallibrary.un.org/record/1630495?ln=en&v=pdf(дата звернення 27.10.2023).

752. Proposal for a Regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts 2021/0106 (COD), 21.4.2021. URL: https:// digital-strategy. ec.europa.eu /en/library/coordinated -plan-artificial-intelligence-2021 -review (дата звернення 09.09.2023).

753. Protection of the Privacy of Individuals Vis-a-vis Electronic Data Banks in the Private Sector: Resolution (73) 22 Adopted by the Committee of Ministers of the Council of Europe on 26 September 1973: and Explanatory Report. URL: https://rm.coe.int/1680502830 (дата звернення 08.10.2023).

754. Quintana E.A. Natural persons, juridical persons and legal personhood. *Mexican Law Review.* 2015. № 8. P. 101-118. URL: https://www.elsevier.es/es-revista-mexican-law-review-123-articulo-natural-persons-juridical-persons-and-S1870057815000062 (дата звернення 05.10.2023).

755. Radical Technologies: The Design of Everyday Life. Adam Greenfield. Verso, 2017. 359 p.

756. Rainie L., Anderson J. Privacy in 2025: Experts' Predictions. USA, Pew Research Center, 2014. URL: http://www.pewinternet.org/2014/12/18/privacy- in-2025-experts-predictions/ (дата звернення 02.10.2022).

757. Rainie L., Anderson J., Albright J. The Future of Free Speech, Trolls, Anonymity, and Fake News Online. Pew Research Center, 2017. 82 p.

758. Radutniy O.E. Criminal Liability of the Artificial Intelligence. Problems of legality. 2017. № 138. P. 132-141. https://doi.org/10.21564/2414-990x.138.105661

759. Rakka J. Freedom and right (not) to know. *Bioethics.* 1998. Vol. 12. №1. P. 50-63.

760. Ranking Digital Rights advances corporate accountability for human rights in the digital age. URL: https://rankingdigitalrights.org/(дата звернення 05.10.2023).

761. Ranchordas S. The Digitalization of Government and Digital Exclusion: Setting the Scene. *University of Groningen faculty of law research paper. Groningen.* 2020. № 30. P. 1-31. URL: https://ssrn.com/abstract=3663051 (дата звернення 15.05.2023).

762. Rausiala K. The Rise of Transnational Networks Conference November 7, 2008 Transnational Networks: Past and Present. *The International Lawyer*. 2009. № 1. 205-209. URL: https:// scholar. smu.edu/cgi/ viewcontent. cgi?article=1248 & context=til (дата звернення 28.12.2023).

763. Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace Date and place of adoption:15 October 2003. Paris, France. URL: https:// www.unesco.org /en/legal-affairs / recommendation-concerning- promotion-and-use- multilingualism-and-universal- access- cyberspace (дата звернення 05.10.2023).

764. Reglitz M. The Human Right to Free Internet Access. *Journal of Applied Philosophy*. 2019. № 37(2). P. 314-331 URL: https://doi.org/10.1111/japp.12395 (дата звернення 05.10.2023).

765. Remarks on Internet Freedom. H.R. Clinton Secretary of State The Newseum Washington, DC January 21, 2010. URL: https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (дата звернення 05.10.2022).

766. Reidenberg J.R. Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review.*1999- 2000. № 52. P. 1315-1371. URL: https://ir.lawnet.fordham.edu/faculty_scholarship/41 (дата звернення 05.07.2023).

767. Redeker D., Gill L., Gasser U. Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. *The International Communication Gazette*. 2018. № 4. P. 302-319. doi:10.1177/1748048518757121. (дата звернення 07.08.2023).

768. Remembrance day. URL: https://twitter.com/RemembranceDay (дата звернення 05.10.2022).

769. Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) 2015. URL: http://www.uniformlaws.org/ shared/docs/ Fiduciary%20 Access%20to% 20Digital%20 Assets/2015_ RUFADAA_ Final%20Act _2016mar8. pdf (дата звернення 05.07.2023).

770. Richards J. Google Could Be Superseded, Says Web Inventor, TIMES ONLINE (London), Mar. 12, 2008. URL: https://www.thetimes.com/sunday-times-100-tech/hardware-profile/article/google-could-be-superseded-says-web-inventor-jnwsctftvc2(дата звернення 08.08.2023).

771. Richards N.M. The Information Privacy Law Project. Georgetown Law Journal. 2006. № 94. P. 1087-1140. URL: https://ssrn.com/abstract=941181 (дата звернення 08.08.2023).

772. Rikke J.F., Marzouki M. Internet Governance and the Reshaping of Global Human Rights Legacy at WSIS+10. *GigaNet Annual Symposium* (November 2015), João Pessoa, Brazil. P. 1-24. URL: https://ssrn.com/abstract_=2809888 (дата звернення 08.08.2023).

773. Ritter J., Mayer A. Regulating data as property: a new construct for moving forward. *Duke Law & Technology Review*. 2018. № 16. P. 220-277. URL: https://scholarship.law.duke.edu/dltr/vol16/iss1/7/ (дата звернення 08.08.2023).

774. Rodrigues R.E. Revisiting the legal regulation of digital identity in the light of global implementation and local difference. Thesis. The University of Edinburgh, 2011. 352 p. URL: https:// era.ed.ac.uk/ bitstream/handle /1842/8942/ Rodrigues2012.pdf ?sequence=2&is Allowed =y (дата звернення 05.11.2023).

775. Rosenblatt B., Trippe W., Mooney S. Digital rights management*:* business *and* technology. John Wiley & Sons. 2001. 316 p.

776. Rossi A. Internet Privacy: Who Sets the Global Standard? *The International Spectator*. 2014. №1. P. 65-80. URL: DOI 10.1080/03932729. 2014.875823.

777. Russell S., Norvig P. Artificial Intelligence: A modern approach, 4th US ed. Pearson education. 2021. Pearson. 1165p. URL: https://dokumen.pub/artificial-intelligence-a-modern-approach-4nbsped-0134610997-9780134610993.html (дата звернення 08.12.2023).

778. Safe Haven URL: https://safehaven.io (дата звернення 07.06.2023).

779. Sarda T., Natale S., Sotirakopoulos N., Monaghan M. Understanding Online Anonymity. *Media Culture & Society*. 2019. № 4. P. 557-564. URL: DOI 10.1177/ 0163443719842074.

780. Sarma A.C., Girão J. Identities in the Future Internet of Things. Wireless Personal Communications. 2009. № 49. P. 353. (дата звернення 08.10.2023).

781. Sehyeon D. Baek Profiles Is Legal? Understanding Phantom Buster's Data Privacy Practices. 2024. URL: https://www. linkedin.com/pulse /data-scraping-

linkedin-profiles-legal-understanding- phantom-baek--ytkkc/ (дата звернення 25.12.2024).

782. Schwab K. The fourth industrial revolution World Economic Forum 2016. URL: https://www. weforum.org/stories/2016/01/ the-fourth-industrial-revolution-what-it-means-and- how-to-respond/ (дата звернення 08.08.2023).

783. Schwartz P.M. The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. *Harvard Law Review.* 2013. № 7. P. 1966-2009.

784. Schwartz A., Robert S.E. Third-Party Beneficiaries and Contractual Networks. *Legal Analysis.* 2015. № 2. P. 325-361. URL: https://scholarship.law.columbia.edu/faculty_scholarship/336 (дата звернення 06.04.2023).

785. Schweighofer E. Vorüberlegungen zu künstlichen Personen: autonome Roboter und intelligente Softwareagenten. in Schweighofer E., Menzel T., Kreuzbauer G. Auf dem Weg zur ePerson. 2001. P. 45-54.

786. Scritto F. What is digital reputation and how to manage it. 2023. URL: https://icaaou.com /what-is-digital-reputation-and-how-to-manage-it/ (дата звернення 06.04.2024).

787. Shields M., Potter M. Austria's highest court to decide whether to allow class action vs Facebook. URL: https://www.reuters.com/article/us-eu-privacy-facebook-schrems-idUSKBN0TC0L220151123 (дата звернення 08.07.2023).

788. Shen X., Wang C., Chen C. Stress and Internet Addiction: Mediated by Anxiety and Moderated by Self-Control. *Psychoogyl Research and Behavior Management*. 2023. № 16. P. 1975-1986. URL: https://doi.org/10.2147/PRBM.S411412

789. Shilina S. What is decentralized identity in blockchain? SEP 03, 2022. URL: https://cointelegraph.com/explained/what-is-decentralized-identity-in-blockchain (дата звернення 06.07.2023).

790. Szoszkiewicz L. Internet Access as a New Human Right? State of the Art on the Threshold of 2020. *Adam Mickiewicz University Law Review*. 2018. № 8. P. 49-62. URL: DOI 10.14746/ppuam.2018.8.03

791. Smed S. Intelligent Software Agents and Agency Law. *Santa Clara High Technology Law Journal.* 1998. № 2. URL: http://digitalcommons.law.scu.edu/chtlj/vol14/iss2/8 (дата звернення 06.04.2023).

792. Smedinghoff T.J. Introduction to Online Identity Management. March 2019. URL: https:// uncitral.un.org/sites/ uncitral.un.org/ files/media-documents/ uncitral/en/ smedinghoff_paper_ introduction_to_identity _management.pdf (дата звернення 06.04.2023).

793. Smit E.G., Van Noort G., Voorveld H.M. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*. 2014. № 32. P. 15-22. URL: https://doi.org/10.1016/j.chb.2013.11.008 (дата звернення 27.12.2023).

794. Smriti B. Three and a Half Degrees of Separation, Facebook Reaserch. 2016. URL: https://research.fb.com/blog/2016/02/three-and-a-half-degrees-of-separation/ (дата звернення 06.08.2023).

795. Solaiman S.M. Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy. *Artificial Intelligence and Law.* 2017. № 2. P. 155-179.

796. Solove D.J. The Myth of the Privacy Paradox. *The George Washington Law Review.* 2021. № 1 (89). P. 1-51. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265(дата звернення 06.09.2022).

797. Solove D.J., Rotenberg M., Schwartz P.M., Information privacy law. 2nd ed. *Aspen Law & Business*. 2005. 1005 p.

798. Solove D.J. The Digital Person: Technology and Privacy in the Information Age. New York University press. 2004. 283 p. URL: https:// ssrn.com /abstract=2899131 (дата звернення 06.08.2023).

799. Sookman B.B. Computer, Internet and electronic commerce terms *judicial, legislative and technical definitions* Thomson Carswell 2003. 363 p. URL: https:// openlibrary.org /books/ OL35716357M/ Computer_ Internet_and_ electronic_commerce_terms#overview (дата звернення 06.04.2023).

800. Sovereignty. URL: https:// dictionary. cambridge.org /dictionary/ english/ sovereignty (дата звернення 06.04.2023).

801. Stewart R., Hinds G. Algorithms of war: The use of artificial intelligence in decision making in armed conflict. October 24, 2023. URL: *https:// blogs.icrc.org /law-and-policy/ 2023/10/24/ algorithms-of- war-use-of-artificial-intelligence-decision-making-armed -conflict/* (дата звернення 06.04.2024).

802. Strahilevitz J.A. Social Networks Theory of Privacy. *University Chicago Law Review*. 2005. № 72. P. 919-988. URL: https://core.ac.uk/ download/ pdf/234 109688 .pdf (дата звернення 13.11.2024).

803. Sullivan C. Digital Identity: An Emergent Legal Concept. University of Adelaide Press, 2011. 162 p. URL: http://www.jstor.org/stable/10.20851/j.ctt1sq5wqb. (дата звернення 07.07.2023).

804. Sullivan C.L. Digital Citizenship and the Right to Identity in Australia. *Federal Law Review*. 2013. № 41, p. 557.-584. URL: https://ssrn.com/abstract=2379240 (дата звернення 07.05.2022).

805. Sullivan C. Digital Citizenship: Digital Identity, Right to Privacy, and the Right to Identity in the United States of America. URL: https://fpf.org/wp-content/uploads/2012/07/Digital-Citizenship-Clare-Sullivan1.pdf(дата звернення 09.05.2023).

806. Suler J.R. Identity Management in Cyberspace. *Journal of Applied Psychoanalytic Studies*. 2002. № 4. P. 455-459 https://doi.org/10.1023/A:1020392231924(дата звернення 06.07.2023).

807. Technology Landscape for Digital Identification. International Bank for Reconstruction and Development. 2018. 95 p. URL: http://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf(дата звернення 07.07.2023).

808. Tehran Unfetters Cellphones, and the Pictures Start Flowing. URL: https:// www. nytimes.com/ 2014/09/03/world/asia /iran-speeds-up- cellphone-connections.html (дата звернення 07.07.2023).

809. Telecommunications Act. Passed 08.12.2004. Riigikogu. URL: https://www.riigiteataja.ee/en/eli/501042015003/consolide (дата звернення 07.05.2023).

810. Sengupta S. Naming Names: Rushdie Wins Facebook Fight. *New-York Times.* November 15, 2011. URL: http://www.nytimes.com/2011/11/15/technology/hiding-or- using-your-name-online-and-who-decides.html?pagewanted=all&_r=0. (дата звернення 07.07.2023).

811. Terpstra G.A. Self VS. Digital Self Graduate Theses. 2016. 69p. URL: https://doi.org/10.31274/etd-180810-5654(дата звернення 12.07.2023).

812. Terms & Conditions. BlaBlaCar 2021. URL: https://blog.blablacar.co.uk/about-us/terms-and-conditions#:~:text=BlaBlaCar%20grants%20you%20a%20non,the%20Platform%20and%20the%20Services. (дата звернення 07.07.2023).

813. Terms and Conditions Second Life. URL: http://secondlife.com/corporate/tos.php (дата звернення 17.08.2023).

814. The California Consumer Privacy Act. CCPA. 2018. URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5(дата звернення 07.07.2022).

815. The charter of human rights and principles for the Internet. Internet Governance Forum United Nations. 4 th edition. 2014. URL: https:// www. ohchr.org/ sites/default/files/ Documents/Issues/Opinion/ Communications/ Internet PrinciplesAndRightsCoalition.pdf (дата звернення 07.12.2023).

816. The Digital fairness Act. New York State Senate S2277. January 19, 2023. URL: https://www.nysenate.gov/legislation/bills/2023/S2277__(дата звернення 07.07.2024).

817. The Montreal Declaration for a responsible development of artificial intelligence. *Montreal Declaration Responsible AI.* 2017. URL: https://www.montrealdeclaration-responsibleai.com/the-declaration_(дата звернення 07.07.2023).

818. The Facial Recognition and Biometric Technology Moratorium Act of 2020. *Congress government*. 2020. URL: https://www.congress.gov/bill/116th-congress/senate-bill/4084. (дата звернення 07.07.2023).

819. The protection of individuals with regard to automatic processing of personal data Convention. № 108. 28.01.1981. URL: https:// www.edps. europa.eu/ data-protection/ our-work/ publications /legislation/ council- europe-convention-no-108-data-protection _en (дата звернення 14.07.2023).

820. The Right to privacy in the digital age. Resolution adopted by the General Assembly on 18 December 2013. [on the report of the Third Committee (A/68/456/Add.2)] 68/167. URL: https://docs.un.org/en/A/68/PV.70 (дата звернення 07.07.2023).

821. The rule of law on the Internet and in the wider digital world. Issue paper published by the Council of Europe Commissioner for Human Rights Executive summary and Commissioner's recommendations 2014. URL: https:// www.statewatch.org/media/ documents/news/2014/dec/coe-hr-comm-rule-of-law -on-the%20 internet- summary. Pdf (дата звернення 07.07.2023).

822. The UN Guiding Principles (UNGPs) on Business and Human Rights. *Resolution 17/4 on 16 June 2011*. URL: https:// www.ohchr.org/ sites/ default/files/ documents/ publications/ Guidingprinciples Businesshr _eN.pdf (дата звернення 08.12.2023).

823. The Uniform Law Commission. Uniform Fiduciary Access to Dig. Assets Act (UFADAA) 2014. URL: http://www.uniformlaws.org/ shared/docs/Fiduciary%20Access%20to%20Digital% 20Assets/2014_ UFADAA _Final.pdf[https://perma.cc/92VC-H9FE]. (дата звернення 07.08.2023).

824. The Power of BigTech and Ethics, C. Veliz. GRC World Forums1 April 2021 URL:https://www.grcworldforums.com/on-demand-content/the-power-of-bigtech-and-ethics-carissa-veliz/1185.article(дата звернення 07.11.2023).

825. Thompson G., Between hierarchies and markets: the logic and limits of network forms of organization. 2003. Oxford, UK: Oxford University Press. 284 pages.

826. Thornhill J. Internet access is both a human right and a business opportunity. *Financial Times*. 29 June 2020. URL: https: //www.ft_.com/content/ 872dc219-d4d8-4896-92d3-7f9d45a5ce90 (дата звернення 07.12.2023).

827. Tikk E. IP addresses subject to Personal data regulation. 2010. P.24-39. URL: https:// www.ccdcoe.org/ uploads/2010/ 01/2.Tikk_IPAddresses SubjecttoPersonalData Regulation.pdf (дата звернення 10.07.2022).

828. Tokareva V. Davydova I., Adamova E. Legal problems of the use of orphan works in digital age. *Juridical Tribune.* 2021. № 11. P. 452-471.

829. Tokareva V. Digital identity as the element of concept of service-oriented state. Doctrina et Usu in Business Law . Contributions to the 12th International Conference Challenges of Business Law in the Third Millennium, November 25, 2022, Bucharest ADJURIS. P. 281-301.

830. Tomalty J. Is There a Human Right to Internet Access? *Philosophy Now.* 2017. № 118. P. 6-8. URL: https:// philpapers.org/rec/TOMITA (дата звернення 05.10.2023).

831. Trottier C. Who Owns your Digital Identity? The Answer May Shock You URL: https:// peer.social /technology/who-owns-your-digital-identity/ (дата звернення 05.10.2023).

832. Transforming Global Internet Access with SpaceX Starlink. June 12, 2024. URL: https://starlinkinstallationpros.com/transforming-global-internet-access-with-spacex-starlink/(дата звернення 05.11.2024).

833. Triggs G. Digital Rights Watch. *State of digital rights.* 2018. P. 4-5. URL: https://digital rightswatch.org.au/wp-content/ uploads/2018/05/ S tate-of-Digital-Rights-Web.pdf (дата звернення 05.10.2023).

834. Trainees Conference Recording – An. An Orwellian Premonition: a discussion on the perils of biometric surveillance. 21.07.2021. URL: https://edps.europa.eu/press-publications/press-news/videos/trainees-conference-recording-orwellian-premonition-discussion_en (дата звернення 15.08.2023).

835. Travers J., Milgram S., An Experimental Study of the Small World Problem. Sociometry. *American Sociological Association.* 1969. № 4 (32). P. 425-443. URL: http://www.jstor.org/stable/2786545 (дата звернення 05.11.2023).

836. Tully S. A Human Right to Access the Internet? Problems and Prospects. *Human Rights Law Review*. 2014. № 2. P. 175-195. URL: https:// academic. oup.com/hrlr/article-abstract /14/2/175/615750. (дата звернення 05.12.2023).

837. Tunis Agenda for The Anformation Society. 18 November, 2005. URL: https:// www. itu.int/net/ wsis/ docs2/tunis/off/6rev1.html (дата звернення 10.07.2023).

838. Turkle S. Cyberspace and Identity. *Contemporary Sociology.* 1999. № 6. P. 643-648.

839. Two US lawyers fined for submitting fake court citations from ChatGPT URL: https://www.theguardian.com/technology/2023/jun/23/two-us-lawyers-fined-submitting-fake-court-citations-chatgpt(дата звернення 12.01.2023).

840. Van Beers B. The Changing Nature of Law's Natural Person: The Impact of Emerging Technologies on the Legal Concept of the Person. *German Law Journal*. 2017. № 18(3). P. 559-594.

841. Van Dijck J. You Have One Identity: Performing the Self on Facebook and LinkedIn. *Media, Culture & Society.* 2013. № 2. P. 199-215. https://doi.org/10.1177/0163443712468605 (дата звернення 17.08.2023).

842. Van Kokswijk J. Legal Aspects of Virtual Identity. International Conference on Cyberworlds 2007. P. 77- 82.

843. Van Kokswijk J. Digital Ego: Social and Legal Aspects of Virtual Identity. *International Journal of Human and Social Science*. 2008. № 9(3). P. 32-43.

844. Van Kokswijk J. Granting Personality to a Virtual Identity. *International Journal of Humanities and Social Sciences*. 2008. № 8. P. 506-514.

845. Via McCann FitzGerald Solicitors. Are IP addresses personal data? Interview with P. Hustinx EDPS. 04.11.2008. URL: http://news.zdnet. co.uk/security/0,1000000189,39540137,00.htm (дата звернення 05.11.2023).

846. Virtual. Meaning. URL: https://dictionary.cambridge.org/(дата звернення 12.11.2023).

847. Vučković R., Kanceljak I. Does the right to use digital content affect our digital inheritance? *EU and comparative law issues and challenges series.* 2019. November. P. 724-746. DOI:10.25234/eclic/9029

848. Wagner M. This virtual politician wants to run for office. November 23, 2017. URL: https://edition.cnn.com/2017/11/23/tech/first-virtual-politician-trnd/index (дата звернення 09.10.2023).

849. White Paper on Artificial Intelligence A European approach to excellence and trust European Commission. 19.2.2020 COM(2020)65. URL: https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf (дата звернення 17.12.2023).

850. Wachter S., Mittelstadt B., Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law.* 2017. № 2 (7). P. 76-99. URL: https://ssrn. com/abstract=2903469(дата звернення 05.11.2023).

851. Wachter S. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *Computer law & security review.* 2018. № 34. P. 436–449.

852. Wadham J., Gallagher C., Chrolavicius N. Blackstone's Guide to the Identity Cards Act. 1st Edition. Blackstone Press. 2006. 300 p.

853. Warren S.D., Brandeis L.D. The Right to Privacy. *Harvard Law Review.* 1890. № 4. P.193-220. URL: https://doi.org/10.2307/1321160

854. Washington could be the first state to rein in automated decision-making. 02.08.2019. URL: https:// www.fastcompany. Com /90302465/ washington-introduces- landmark- algorithmic -accountability-laws (дата звернення 07.07.2023).

855. Wasko M., Faraj S. Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*. 2005. № 29 (1). P. 35–57.

856. Web H.A. Governance framework for algorithmic accountability and transparency. 2019. URL: https:// www. semanticscholar.org /paper/A-governance-framework-for-algorithmic-and-Webb/ 391a7aa2203cf3c17d97 5d66391f65f40b6 f401e (дата звернення 27.11.2023).

857. Webb S. Houston teachers to pursue lawsuit over secret evaluation system. May 11, 2017. URL: https:// www. houstonchronicle. com /news/ houston-texas/ houston/ article/ Houston-teachers- to-pursue-lawsuit- over-secret-11139692. php (дата звернення 20.10.2022).

858. Wein L. The Responsibility of Intelligent Artifacts: Toward an Automation Jurisprudence. *Harvard Journal of Law & Technology.* 1992. Vol. 6. P. 103-154.

859. Weitzenboeck E.M. Electronic Agents and the Formation of Contracts. *International Journal of Law and Information Technology*. 2001. № 3. Vol. 9. P. 204-234. URL: https://ssrn.com/abstract=2173226_(дата звернення 12.05.2023).

860. Westin A. Privacy and Freedom. *Washington and Lee Law Review.* 1967. Vol 25. №1. P. 166-170. URL: https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20 (дата звернення 20.11.2022).

861. West B.J., Scafetta N. Disrupted networks: from physics to climate change.World Scientific Publishing Company. 2010. 316 p. https://doi.org_/10.1142/ 7714

862. Wet bescherming persoonsgegevens Regeling vervallen per 25-05-2018. URL: https://wetten.overheid.nl/BWBR0011468/2018-05-01(дата звернення 20.11.2023).

863. Wettig St., Zehendner E. The Electronic Agent: A Legal Personality under German Law? 2003 URL: https:// www.researchgate. net/ publication/228978997 _(дата звернення 24.05.2023).

864. What is mathwashing? URL: https:// www. mathwashing. com (дата звернення 20.10.2024).

865. What is the Online Reputation Management? 12.09.2023. URL: https://smowl.net/en/blog/online-reputation-management/ _(дата звернення 20.12.2023).

866. White paper On Artificial Intelligence – A European approach to excellence and trust. 19.02.2020. URL: https://ec.europa.eu /info/sites/default/files/ commission-white-paper-artificial- intelligence-feb2020_en.pdf _(дата звернення 24.05.2023).

867. White A. IP Addresses Are Personal Data, E.U. Regulator Says. 22.01.2008. URL: www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html _(дата звернення 27.05.2023).

868. Who Expert Advisory Committee on Developing Global Standards for Governance and Oversight of Human Genome Editing Report of the first meeting Geneva, Switzerland.18.03.2019. URL: https:// www.who.int/__publications /i/item/WHO-SCI-RFH-2019-01 _(дата звернення 20.05.2023).

869. Wiese G. Gibt es ein Recht auf Nichtwissen? Dargestellt am Beispiel der genetischen Veranlagung von Arbeitnehmern. In: Festschrift für Hubert Niederländer zum 70. Geburtstag. 1991. P. 475-488.

870. Willson M. Community in the Abstract: A Political and Ethical Dilemma? Virtual Politics: Identity and Community in Cyberspace / Ed. By D. Holmes. London: Sage, 1997. 256 p.

871. Wilson R.E., Gosling S.D., Graham L.T. A Review of Facebook Research in the Social Sciences. *Perspectives on Psychological Science.* 2012. № 3. P. 203–220.

872. Wisman T.H. Privacy, Data Protection and E-Commerce. *A Lodder and A Murray (eds), EU Regulation of E-Commerce.* 2017. Chapter 12. 349-382. URL: https:/ /doi.org/10.4337 /978178536 9346

873. Wiszniewski D., Coyne R. Mask and Identity: The Hermeneutics of Self-Construction in the Information Age. Building Virtual Communities: Learning and change in cyberspace / *K.A. Renninger, W. Shumar* (eds.). Cambridge University Press, 2002. P. 191-214.

874. Wooldridge M., Jennings N. Intelligent Agents: Theory and Practice. *Knowledge Engineering Review*. 1995. Vol. 10. № 2. URL: https:// www.cs. cmu.edu/ ~motionplanning/papers/ sbp_papers/ integrated1/ woodridge_ intelligent_ agents.pdf (дата звернення 20.11.2022).

875. World Food Program. URL: https:// www .wfp .org/ news/ blockchain - against -hunger -harnessing -technology-support-syrian-refugees (дата звернення 20.05.2023).

876. Wynn M., Tillotson K., Kao R. Sexual Intimacy in the Age of Smart Devices: Are We Practicing Safe IoT? Workshop on Internet of Things Security and Privacy. 2017. p. 25-30. doi: 10.1145/3139937.3139942. _(дата звернення 20.05.2023).

877. Yahoo gives dead Marine's family e-mail info. 21.04.2005. URL: https://www. nbcnews. com/id/wbna7581686_(дата звернення 20.05.2023).

878. Yang S. As China shuts out the world, internet access from abroad gets harder too. June 23, 2022. URL: https://www.latimes.com/ world-nation/story/2022-06-23/china-great-firewall-foreign- domestic-virtual-censorship_(дата звернення 20.05.2023).

879. Yes, You Really Can Do a Utah Virtual Wedding Online. URL: https://utahofficiant.com/online-weddings-in-uta _ (дата звернення 20.06.2024).

880. Your digital reputation URL: https:// www. esafety.gov.au /key-issues/ staying- safe/ digital -reputation (дата звернення 20.05.2024).

881. Zankl W. E-Commerce-Gesetz. 2 Auflage. 2016. 560p.

882. Zarsky T. Z. Online Privacy, Tailoring, and Persuasion, in Privacy and Technologies of identity: a Cross-Disciplinary conversation. K. Strandburg, D.S Raicu, eds., 2006. Chapter. 12. P. 209-224. URL: https://ssrn.com/abstract=946428_(дата звернення 27.11.2022).

883. Zenos A. Artificial Intelligence and Data Protection. 2022. URL: https:// towardsdatascience .com/artificial- intelligence-and-data-protection -62b333180a27 _(дата звернення 20.05.2023).

884. Zidar P., Miha M. Personal brand. International Conference on Organizational Science Development Internationalization and cooperation. 2015. P.1351-1359. URL: https://www.researchgate.net/publication/274073688_(дата звернення 20.11.2022).

885. Ziegler S. Internet of Things Security and Data Protection. 1st ed. Edition. Springer International Publishing, 2019. 232 p. URL: https://doi.org/10.1007/978-3-030-04984-3.

886. Zimmerman E., Machine Minds: Frontiers in Legal Personhood. February. 2015. P. 1-43. URL: https://ssrn.com/abstract=2563965 (дата звернення 20.04.2023).

887. Zitter L. What Are Intelligent Virtual Agents (IVAs)? 12.04.2022. URL: https://www.cmswire.com/customer-experience/what-are-intelligent-virtual-agents-ivas/ (дата звернення 20.12.2022).

888. Zoltan M. Web Scrapers Claim to Possess and Sell Personal Data on 1.5 Billion Facebook Users on a Hacker Forum. 30 November, 2022 URL: https://www. privacyaffairs.com/ facebook-data-sold-on-hacker- forum/ (дата звернення 20.06.2023).

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Наукові, праці в яких опубліковані основні наукові результати дисертації:

1. Токарева В.О. Наслідки порушення прав інтелектуальної власності китайськими товаровиробниками. *Часопис цивілістики.* 2016. № 20. С. 202-206. URL: http://clj.nuoua.od.ua/archive/20/43.pdf

2. Токарева В.О. Авторське право у цифрову добу. *Часопис цивілістики.* 2017. №26. С. 93-98. URL: http://clj.nuoua.od.ua/archive/26/22.pdf

3. Токарева В.О. Інтелектуальна власність КНР: на шляху інновацій. *Науковий Вісник МГУ.* 2018. № 32. С. 53-56. URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc32/14.pdf

4. Токарева В.О. Щодо питання творчості та штучного інтелекту. *Прикарпатський юридичний вісник.* 2018. № 1(22). С. 55-58. URL: http://pjv.nuoua.od.ua/v1_2018/15.pdf

5. Токарева В.О. Онлайн платформи: виклик авторському праву у цифрову добу. *Часопис цивілістики.* 2018. № 29. С. 107-111. URL: http://clj.nuoua.od.ua/archive/29/23.pdf

6. Токарева В.О. Обчислювальна творчість (щодо питання творчості штучного інтелекту). *Часопис цивілістики*. 2018. № 30. С. 38-43. URL: http://clj.nuoua.od.ua/archive/30/10.pdf

7. Токарева В.О. Щодо питання інформаційної природи авторського права. *Часопис цивілістики.* 2019. № 33. С. 61-66. URL: http://clj.nuoua.od.ua/archive/33/13.pdf

8. Токарева В.О. Умови охороноздатності об’єктів авторського права. *Приватне та публічне право.* 2019. № 3. 39-43. URL: http://www.pp-law.in.ua/archive/3_2019/11.pdf

9. Токарева В.О. Похідні твори у галузі сучасного мистецтва. *Науковий вісник публічного та приватного права.* 2019. № 6. С. 35-40. URL: http://nvppp.in.ua/vip/2019/6/7.pdf

10. Токарева В.О. Сумлінне використання та похідні твори у сучасному мистецтві. *Таврійський національний університет імені В.І. Вернадського.* 2020. Т. 31 (70). № 2. С. 121-125. URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_1/25.pdf

11. Токарева В.О. Щодо питання захисту прав інтелектуальної власності. *Часопис Цивілістики.* 2020. №. 36. 51-56. URL: http://clj.nuoua.od.ua/archive/36/11.pdf

12. Токарева В.О. Формування категорії «віртуальна ідентичність» у мережі Інтернет. *Часопис Цивілістики*. 2022. № 45. С. 63-67. URL: http://chascyvil.onua.edu.ua/index.php/chc/article/view/468/511

13. Токарева В.О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 3. С. 47-52. URL: http://apnl.dnu.in.ua/3_2022/8.pdf

14. Токарева В.О. Окремі питання реалізації права на видалення. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 4. С. 43-47. URL: http://apnl.dnu.in.ua/4_2022/8.pdf

15. Токарева В.О. Щодо визначення персональних даних в умовах Євроінтеграційних процесів. *Південноукраїнський правничий часопис.* 2022. № 4. Том 3. С. 169-174 URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_3/28.pdf

16. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Публічне та приватне право.* 2022. № 4. С. 35-40. URL: http://pp-law.in.ua/archive/4_2022/6.pdf

17. Токарева В.О. До питання прийняття рішень із застосування алгоритмів**.** *Публічне та приватне право.* 2023. № 1. С. 30-35. URL: http://pp-law.in.ua/archive/1_2023/5.pdf

18. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики.* 2023. № 49. С. 32-37. URL: http://clj.nuoua.od.ua/archive/49/5.pdf

19. Токарева В.О. Правове регулювання застосування систем віддаленої біометричної ідентифікації в ЄС. *Публічне та приватне право.* 2023. № 2. С. 3-8. URL: http://pp-law.in.ua/archive/2_2023/1.pdf

20. Токарева В. Реалізація сімейної правоздатності фізичної особи за допомогою мережі Інтернет. *Юридичний бюлетень.* 2023. № 29. С. 134-141. URL: http://www.lawbulletin.oduvs.od.ua/archive/2023/29/14.pdf

21. Токарева В.О. Порушення прав на торговельні марки в мережі Інтернет. Юридичний науковий електронний журнал. 2023. № 10. С.141-144. URL: http://www.lsej.org.ua/10_2023/32.pdf

22. Токарева В.О. Окремі питання управління майном фізичної особи**.** *Юридичний науковий електронний журнал.* 2024. № 4. С. 129-131. URL: http://www.lsej.org.ua/8_2024/30.pdf

23. Токарева В.О. До питання права на зображення (голограму) фізичної особи після смерті в умовах поширення технологій ШІ. *Часопис цивілістики.* 2024. № 54. С. 43-48. URL: http://clj.nuoua.od.ua/archive/54/8.pdf

24. Токарева В.О., Личко В.С. Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С. 848 -851. URL: http://www.lsej.org.ua/4_2024/209.pdf

25. Токарева В.О., Личко В.С. Спадкування об’єктів в мережі Інтернет: досвід західних держав. *Часопис цивілістики.* 2024. № 53. С. 41-46. URL: http://clj.nuoua.od.ua/archive/53/9.pdf

26. Давидов І.В., Токарева В.О. Захист права на повагу до честі та гідності, ділової репутації, публічних осіб. *Держава та регіони. Серія Право.* 2022. № 1 (75). С. 131-135. URL: http://www.law.stateandregions.zp.ua/archive/1_2022/22.pdf

27. Давидова І.В. Токарева В.О. Цифрова нерівність. Цифрова нерівність і право на доступ до Інтернету. *Юридичний вісник.* 2024. № 6. С. 68-75. URL: http://yurvisnyk.in.ua/v6_2024/10.pdf

Наукові праці, статті у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection та Scopus:

28. Nekit K., Tokareva V., Zubar V. Artificial intelligence as a potential subject of property and intellectual property relations. *Ius Humani. Law Journal.* 2020. № 9 (1). P. 231-250. URL: https://doi.org/https://doi.org/10.31207/ih.v9i1.227

29. Tokareva V. Davydova I., Adamova E. Legal problems of the use of orphan works in digital age. *Juridical Tribune.* 2021. № 11. P. 453-471. URL: http://www.tribunajuridica.eu/arhiva/An11v3/3.%20Tokareva%20Davydova%20Adamova.pdf

30. Davydova I., Zhurylo S., Tomina V., Fuchedzhi V., Tokareva V. Legal aspects of the regulation of social relations with the participation of Artificial Intelligence. *Revista De La Universidad Del Zulia*. 2022. № 13 (38). P. 487-500. DOI: http://dx.doi.org/10.46925//rdluz.38.28

31. Davydova I., Nahnybida V., Adamova O., Zhurylo S., Tokareva V. Blockchain and civil proceedings: points of convergence. *DIXI*. 2022 (2023). № 25(1). P. 1–20. URL: https://revistas.ucc.edu.co/index.php/di/article/view/4637

32. Davydova I., Bernaz-Lukavetska O., Tokareva V., Andriienko I., Tserkovna O. Freedom of contract in the digital age and its implementation in modern technologies: theory and practice. *International Journal of Computer Science and Network Security*. 2022. № 12 (21). P. 544-548. URL: http:// paper.ijcsns.org/07_book/202112/20211275.pdf

Наукові статті у зарубіжних періодичних виданнях юридичного напряму:

33. Токарева В.О. Проблемні питання творчості в умовах цифрової доби. *European political and law discourse.* 2019. № 2. С. 123-128. URL: https://eppd13.cz/wp-content/uploads/2019/2019-6-2/eppd_2019_6_2.pdf

34. Токарева В.О. Окремі аспекти сирітських творів в умовах інтеграційних процесів. *Jurnaluljuridic.* 2019. № 3. С. 97-101. URL: http://www.jurnaluljuridic.in.ua/archive/2019/3/part_1/22.pdf

35. Токарева В.О. Обчислювальна (Алгоритмічна) творчість: постановка проблеми. *Visegrad Jurnal on Human Rights.* 2019. № 2. (V.2). С. 150-155. URL: https://journal-vjhr.sk/wp-content/uploads/2020/12/Vyshegrad-2_2019_Tom-2.pdf

36. Токарева В.О. Окремі питання легалізації сирітських творів. *Recht der Osteuropäischen Staaten (ReOS).* 2019. №1. С. 197-201. URL: https://www.uni-goettingen.de/de/document/download/ca207b2c626da0c3a651dab3e413069e.pdf/ReOS%2001%20aus%202019.pdf

Наукові праці які засвідчують апробацію матеріалів дисертації:

37. Токарева В.О. Дискусійні питання алгоритмічної творчості. *Розвиток державності та права в Україні реалії та перспективи*: матеріали міжнародної науково-практичної конференції. (м. Львів, 20-21 вересня 2019 р.). Львів: Західноукраїнська організація «Центр правничих ініціатив», 2019. С. 42-46.

38. Токарева В.О. Дотримання GDPR в умовах COVID-19. *Інформаційні технології в умовах оновлення цивільного законодавства*: матеріали. Всеукр. кругл. столу (м. Одеса, 13 черв. 2020 р.) За заг. ред. О. І. Харитонової, Є. О. Харитонова. Одеса: Фенікс, 2020. С. 60-62.

39. Токарева В.О. Щодо окремих питань творчості штучного інтелекту. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-ти річчя проголошення незалежності України та 25-ти річчя прийняття Конституції України):* матеріали Міжнародної науково-практичної конференції (21 травня 2021 р.). Одеса: Причорноморська фундація права. С. 352-356.

40. Токарева В.О. Проблемні аспекти творчості в епоху цифрових трансформацій. *Взаємодія громадянського суспільства, особи і держави:* вектор удосконалення: матеріали Міжнародної науково-практичної конференції. (м. Київ, 22 червня 2021р.). Київ: Київський регіональний центр НАПрН, 2021. С. 179-182.

41. Токарева В.О. Проблеми легалізації сирітських творів в умовах інформаційного суспільства. *Проблеми та стан дотримання і захисту прав людини в Україні*: Матеріали міжнародної науково-практичної конференції (м. Львів, 20–21 серпня 2021 р.). Львів: Західноукраїнська організація «Центр правничих ініціатив», С. 31-34.

42. Токарева В.О. Окремі питання реалізації права на творчість особами засудженими до позбавлення волі. *Юридична наука: виклики і сьогодення*: матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 11–12 червня 2021 р.). Одеса: ГО «Причорноморська фундація права», 2021. С. 49-52.

43. Токарева В.О. Еволюція концепту творчості та розвитку інновацій в КНР. *Сучасне правотворення: питання теорії та практики*: Матеріали міжнародної науково-практичної конференції (м. Дніпро, 4–5 червня 2021 р.). Дніпро: ГО «Правовий світ», 2021. С. 51-54.

44. Токарева В.О. До питання результатів інтелектуальної діяльності та штучного інтелекту. *Особливості розвитку законодавства України у контексті євроінтеграційних процесів*: міжнародна науково-практична конференція (м. Харків, 4–5 червня 2021 р.). Харків: Східно-українська наукова юридична організація, 2021. С. 68-71.

45. Токарева В.О. Результати творчості сгенеровані штучним інтелектом. *Сучасний вимір держави і права*: матеріали міжнародної науково-практичної конференції (м. Львів, 18–19 червня 2021 р.). Львів: Західноукраїнська організація «Центр правничих ініціатив», 2021. С. 102-106.

46. Токарева В.О. Право на свободу вираження творчості. *Актуальні питання реформування правової системи України*: матеріали міжнародної науково-практичної конференції (м. Дніпро, 2–3 липня 2021 р.). Дніпро: ГО «Правовий світ», 2021. С. 17-20.

47. Токарева В.О. Окремі аспекти вираження творчості в умовах цифрових трансформацій. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI*

століття (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права): у 2 т.: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса: Видавничий дім «Гельветика», 2022. Т. 2. 2022 . С. 659-662.

48. Токарева В.О. Деякі питання щодо категорії «віртуальна ідентичність» у мережі Інтернет. *Integration of Education, Science and Business in Modern Environment: Summer Debates*: Proceedings of the 4th International Scientific and Practical Internet Conference (August 15-16, 2022.). Dnipro: FOP Marenichenko V.V. С. 67-69.

49. Токарева В.О. Деякі питання щодо категорії «віртуальна ідентичність» у мережі Інтернет. *Розвиток громадянського суспільства як необхідна складова європейської інтеграції України*: матеріали Всеукраїнської науково -практичної конференції (м. Київ, 06 жовтня 2022 р.). Львів-Торунь: Liha-Pres, 2022. С. 292-295. DOI https://doi.org/10.36059/978-966-397-271-8-78.

50. Токарева В.О. Право на видалення та право на чистий цифровий лист. *Правове регулювання суспільних відносин: перспективні напрями на шляху до сталого розвитку*: матеріали Міжнародної науково-практичної конференції (м. Київ, 28-29 жовтня 2022 р.). Львів: Торунь: Liha-Pres, 2022. С. 46-50.

51. Токарева В.О. Щодо питання цифрової ідентичності в умовах війни. *Приватне право в умовах війни*: матеріали всеукр. наук. конф. (Одеса, 15 листоп. 2022 р.). за заг. ред.: д.ю.н., проф. Є. Харитонова, д.ю.н., проф. І. Давидової. Одеса: НУ «Одеська юридична академія. 2022. С. 111-116. URL: https://hdl.handle.net/11300/25131

52. Tokareva V. Digital identity as the element of concept of service-oriented state. *International Conference Challenges of Business Law in the Third Millennium* (Bucharest, November 25, 2022). Doctrina et Usu in Business Law. Contributions to the 12th. Bucharest: ADJURIS. P. 281-301.

53. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Становлення та розвиток правової держави: проблеми теорії та практики:* Матеріали XV міжнародної науково-практичної конференції, що присвячена

102-річчю Національного університету кораблебудування імені адмірала Макарова, м. Миколаїв. 28–29 грудня 2022 р. Львів-Торунь: Liha-Pres, 2022. С. 351-364.

54. Токарева В.О. Фізична особа в мережі Інтернет. *Актуальні проблеми протидії корупції в Україні в умовах воєнного стану*: матеріали Міжнародної науково-практичої конференції (м. Рівне, 14 березня 2023 року). Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука. Львів: Торунь: Liha-Pres, 2023. 176 с. С. 16-19.

55. Токарева В.О. До питання виникнення правосуб'єктності фізичної особи у мережі Інтернет. *І Міжнародна науково-практична конференція Таврійського національного університету до 160-ї річниці від дня народження В. І. Вернадського:* матеріали Міжнародної науково-практичної конференції, 16-17 березня 2023 р., м. Київ. Частина 1. Львів Торунь: Liha-Pres, 2023. С. 57-61.

56. Токарева В.О. Правове регулювання прийняття рішень із використанням алгоритмів. *Topical issues of modern jurisprudence*: International scientific conference proceedings (April 5–6, 2023. Częstochowa, the Republic of Poland). Riga, Latvia: «Baltija Publishing», 2023. С. 84-88.

57. Токарева В.О. До питання реалізації права відмовитися від ознайомлення із результатами медичних досліджень (право не знати). *Гармонізація законодавства України з правом Європейського Союзу: реалії та перспективи*: Всеукраїнська науково-практична конференція (м. Запоріжжя, 18 травня 2023 р.). Львів-Торунь: Liha-Pres, 2023. С. 169-173.

58. Токарева В.О. До питання прийняття юридично значущих рішень із застосування алгоритмів. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень*: у 2 т.: матеріали Міжнар. наук.- практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редак- цією С. В. Ківалова. Одеса: Юридика, 2023. – Т. 2. С. 534-537.

59. Токарева В.О. Правове регулювання транскордонної обробки персональних даних між ЄС та США. *Римське право і сучасність: актуальні*

проблеми оновлення цивільного законодавства: матер. Всеукр. наук. конф. (м. Одеса, 25 травня 2023 р.) [Електронне видання] / упоряд.: І. Давидова, М. Лєсняков ; за заг. ред. д.ю.н., проф. Є. О. Харитонова. Одеса, 2023. С. 80-85.

60. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень в США. *Проблеми цивільного права у постпандемічну добу*: матер. круг. столу (м. Одеса, 26 травня 2023 р.) [Електронне видання] / укл.: І.В. Давидова, О.В. Шамота; за ред.: Є.О. Харитонова, І.В. Давидової; Нац. ун-т «Одес. юрид. академія». Одеса, 2023. С. 60-64.

61. Токарева В.О. До питання персонанальних даних за законодавством ЄС. *Legal science, legislation and law enforcement: traditions and new European approaches*: International scientific conference proceedings (Wloclawek, May 29-30, 2023). Riga, Latvia: «Baltija Publishing», 2023. 124 pages. С. 39-43.

62. Токарева В.О. До питання дистанційної біометричної ідентифікації. *Восьмі Таврійські юридичні наукові читання:* матеріали міжнародної науково-практичної конференції (м. Київ, 16–17 червня 2023 р.). Львів –Торунь: Liha-Pres, 2023. С.62-66.

63. Токарева В.О. Окремі питання збору та обробки геномної інформації людини. *Договори в умовах миру та війни (до 90-річчя з дня народження В. Луця)*: матеріали Всеукр. наук. конф. [Електронне видання] / за заг. ред. Є. Харитонова, І. Давидової; НУ «Одес. юрид. академія». Одеса: Фенікс, 2023. С. 52-57. URL: https://hdl.handle.net/11300/27420

64. Токарева В.О. До питання «persona» за римським правом. *Цивілістичні проблеми спортивного права*: матеріали Круглого столу, (Одеса, 28.10.2023 р.). [Електронне видання] / за заг. ред.: Є. Харитонова, І. Давидової, М. Ткалича; Нац. ун-т «Одес. юрид. академія». Одеса: Фенікс, 2023. С. 41-43. URL: https://hdl.handle.net/11300/27371

65. Токарева В.О. До питання репутації у мережі Інтернет. *Європейські орієнтири розвитку України*: науково-практичний вимір в умовах воєнних

викликів: матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. Одеса : Фенікс, 2024. С. 591-594.

66. Токарева В.О. До питання цифрової ідентичності та анонімізованих даних. *Римське право і сучасність: реалізація і захист речових прав в умовах воєнного стану*: матеріали Всеукр. наук. конф. (Одеса, 25 трав. 2024 р.) [Електронне видання] / за заг. ред.: Є. Харитонова, І. Давидової, В. Зубара; НУ «Одес. юрид. академія». Одеса: Фенікс, 2024. С. 11-114.

67. Токарева В.О. До питання цифрового громадянства. *Одеські грудневі цивілістичні читання: приватне право, як концепт в умовах війни, людський вимір*: матеріали Всеукр. наук. конф. (Одеса, 12 груд. 2024 р.) [Електронне видання] / за заг. ред.: д.ю.н., проф. Є. Харитонова, д.ю.н., проф. І. Давидової; НУ «Одес. юрид. академія». Одеса: Фенікс, 2025. С. 71-75. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/a2cd872f-d57a-4558-adaa-2cb9f2969520/content

Наукові праці, які додатково відображають наукові результати дисертації:

68. Токарева В.О. Зловживання цивільним правом та право на інформацію. Права приватної особи в умовах пандемії COVID-19: проблеми здійснення і захисту: монографія / Є.О. Харитонов, О.І. Харитонова, К.І. Бєляков; Є.О. Харитонова, О.І. Харитонової, К.Г. Некіт. Одеса: Гельветика, 2020. С. 194-204.

69. Токарева В.О. Обмеження майнових прав інтелектуальної власності у сфері охорони здоров’я. Приватні та публічні інтереси в умовах COVID-19: колізії та правові шляхи вирішення. колективна монографія; за ред. Харитонова Є.О., Харитонова О.І., Булеца С.Б. Одеса 2021. С. 279-293.

70. Токарева В.О. Розвиток цифрової ідентичності як елементу сервісної держави в умовах війни. Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: монографія [Електронне видання] / за ред.: Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт; упор.-укл. Ю.С. Маршук; НУ «Одеська юридична академія». Одеса: Фенікс, 2023. С 86-97.

71. Токарева В.О. Віртуальна ідентичність як проекція фізичної особи у мережі Інтернет. The European dimension of modern legal science: Scientific monograph. Riga, Latvia: Baltija Publishing, 2022. С. 406-418.

72. Токарева В.О. Анонімність в мережі Інтернет. Law in the postmodern epoch: general characteristics and manifestation particularities in separate law branches: Scientific monograph. Riga, Latvia: Baltija Publishing, 2023. С. 6-1-617.

73. Токарева В.О. Інформаційна приватність за законодавством ЄС: виклики та перспективи. Modern paradigm of public and private law amidst sustainable development: Scientific monograph. Vol. 2. Riga, Latvia: Baltija Publishing, 2023. С. 295-310.

Відомості про апробацію результатів дисертації

Результати дослідження обговорено на засіданнях кафедри цивільного права та кафедри права інтелектуальної власності і патентної юстиції Національного університету «Одеська юридична академія» та на засіданні Південного регіонального центру НАПрН України. Основні положення дисертації були апробовані на 31 науковому заході, а саме: Міжнародній науково-практичній конференції «Розвиток державності та права в Україні реалії та перспективи» (м. Львів, 20 вересня 2019 р.); Всеукраїнському круглому столі «Інформаційні технології в умовах оновлення цивільного законодавства» (м. Одеса, 13 червня 2020 р.); Міжнародній науково-практичній конференції «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру» (м. Одеса, 21 травня 2021 р.); Міжнародній науково-практична конференція (м. Київ, 22 червня 2021 р.); Міжнародній науково-практичній конференції Юридична наука: виклики і сьогодення» (м. Одеса, 11 червня 2021 р.); Міжнародній науково-практичній конференції «Сучасне правотворення: питання теорії та практики»(м. Дніпро, 4 червня 2021 р.); Міжнародній науково-практичній конференції «Особливості розвитку законодавства України у контексті євроінтеграційних процесів» (м. Харків, 4 червня 2021 р.);

Міжнародній науково-практичній конференції «Сучасний вимір держави і права» (м. Львів, 18 червня 2021 р.); Міжнародній науково-практичній конференції «Актуальні питання реформування правової системи України» (м. Дніпро, 2 липня 2021 р.); Міжнародній науково-практичній конференції «Актуальні питання правової теорії та юридичної практики» (м. Одеса, 13 серпня 2021 р.); Міжнародній науково-практичній конференції «Проблеми та стан дотримання і захисту прав людини в України» (м. Львів, 20 серпня 2021р.); Міжнародній науково-практичній конференції «Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (м. Одеса, 17 червня 2022 р.); Міжнародній науково-практичній інтернет-конференції «International Scientific and Practical Internet Conference «Integration of Education, Science and Business in Modern Environment» (м. Дніпро, 15 серпня 2022 р.); Всеукраїнській науково-практичній конференції «Розвиток громадянського суспільства як необхідна складова європейської інтеграції України» (м. Київ, 6 жовтня 2022 р.); Міжнародній науково-практичній конференції «Правове регулювання суспільних відносин: перспективні напрями на шляху до сталого розвитку» (м. Київ, 28 жовтня 2022 р.); Всеукраїнській науковій конференції «Приватне право в умовах війни» (м. Одеса, 15 листопада 2022 р.); 12th International Conference Challenges of Business Law in the Third Millennium (Bucharest, 25 November 2022); Міжнародній науково-практичної конференції, присвяченій 102-річчю Національного університету кораблебудування імені адмірала Макарова «Становлення та розвиток правової держави: проблеми теорії та практики» (м. Миколаїв, 28 грудня 2022 р.); Міжнародній науково-практичній конференції «Актуальні проблеми протидії корупції в Україні в умовах воєнного стану» (м. Рівне, 14 березня 2023 р.); Міжнародній науково-практичній конференції Таврійського національного університету до 160-ї річниці від дня народження В. І. Вернадського (м. Київ, 16 березня 2023 р.); International scientific conference «Topical issues of modern jurisprudence»: conference proceedings (Częstochowa, 5 April 2023); Всеукраїнській науково-практичній конференції «Гармонізація

законодавства України з правом Європейського Союзу: реалії та перспективи» (м. Запоріжжя, 18 травня 2023 р.); Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень» (м. Одеса, 19 травня 2023 р.); Всеукраїнській науково-практичній конференції «Римське право і сучасність: актуальні проблеми оновлення цивільного законодавства» (м. Одеса, 25 травня 2023 р.); Круглому столі «Проблеми цивільного права у постпандемічну добу» (м. Одеса, 26 травня 2023 р.); International scientific conference «Legal science, legislation and law enforcement: traditions and new European approaches» (Wloclawek, 29 May 2023); Міжнародній науково-практичній конференції "Восьмі Таврійські юридичні наукові читання" (м. Київ, 16 червня 2023 р.); Круглому столі «Цивілістичні проблеми спортивного права» (м. Одеса, 28 жовтня 2023 р.); Всеукраїнській науковій конференції «Договори в умовах миру та війни (до 90-річчя з дня народження В. Луця)» (м. Одеса, 1 грудня 2023 р.); Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів» (м. Одеса, 26 квітня 2024 р.); Всеукраїнській науковій конференції «Римське право і сучасність: реалізація і захист речових прав в умовах воєнного стану» (м. Одеса, 25 травня 2024 р.); Всеукраїнській науковій конференції «Одеські грудневі цивілістичні читання: приватне право, як концепт в умовах війни, людський вимір» (м. Одеса, 12 грудня 2024 р.).

Додаток Б

«ЗАТВЕРДЖУЮ»
Ректор Національного університету
«Одеська юридична академія»
Професор Тодоцак О.В.

«13» квітня 2025 року

АКТ

про впровадження результатів дисертаційного дослідження докторської дисертації Токаревої Віри Олександрівни на тему «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» за спеціальністю 12.00.03 – «цивільне право і цивільний процес; сімейне право; міжнародне приватне право» в навчальну та науково-дослідну діяльність Національного університету «Одеська юридична академія»

Комісія у складі: голови – проректора з наукової роботи Національного університету «Одеська юридична академія», професора Мінаса Аракеляна,

членів комісії: проректора з навчальної роботи Національного університету «Одеська юридична академія», професора Галини Ульянової, начальника навчально-методичного відділу Національного університету «Одеська юридична академія» Людмили Кузнецової, декана факультету цивільної та господарської юстиції, Національного університету «Одеська юридична академія», доцента Євгена Хижняка, завідувача кафедри цивільного права Національного університету «Одеська юридична академія», професора Євгена Харитонова, склали цей акт про те, що результати дисертаційного дослідження Токаревої Віри Олександрівни на тему «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.03 – цивільне право і цивільний процес; сімейне право; міжнародне приватне право використовується у навчальному процесі Національного університету «Одеська юридична академія» при викладанні навчальних дисциплін: «Цивільне право», «Цивільне та сімейне право України», «Захист персональних даних», а також у науково-дослідній роботі студентів, аспірантів та науковців.

Були враховані положення дисертації про необхідність розширити обсяг матеріалу, що викладається у рамках навчальної дисципліни «Цивільне право» та «Цивільне та сімейне право України» зокрема, щодо розгляду питань вивчення специфіки правосуб'єктності фізичної особи, та появи нових цифрових прав обумовлених розвитком мережі Інтернет та інформаційно комунікаційних систем.

Положення дисертації були враховані під час викладання курсу «Захист персональних даних», зокрема врахована поява нових цифрових прав, виникнення проблем пов'язаних із маніпуляціями із даними та потребою забезпечення прозорості та визначеності реалізації та захисту прав фізичних осіб від дискримінації в умовах поширення автоматизованих систем, предикативної аналітики та технологій Великих даних.

Використання зазначених результатів дослідження дозволить більш повно та грунтовно викладати та засвоювати матеріали вищезазначених навчальних дисциплін та надасть студентам Національного університету «Одеська юридична академія» можливість вивчити особливості визначення поняття зміст у та реалізації цивільної правосуб'єктності фізичної особи в мережі в Інтернет, яка несе істотне наукове та практичне значення; розглянути концептуальні підходи до розуміння мережі як чинника який впливає на уявлення про права людини у мережі Інтернет; визначити права на цифрову ідентичність в мережі Інтернет; розглянути підходи до визначення єдиної цифрової ідентичності фізичної особи в мережі Інтернет; специфіки проведення ідентифікації фізичної особи у відносинах у мережі Інтернет; проаналізувати особливості ідентифікуючих ознак фізичної особи у відносинах у мережі Інтернет; визначити специфіку виникнення та припинення правоздатності та дієздатності фізичної особи в мережі Інтернет; проаналізувати зміст цивільної правоздатності фізичної особи в мережі Інтернет; визначити вплив автоматизованих систем на особливості реалізації правоздатності та дієздатності в мережі Інтернет; дослідити специфіку дієздатності фізичної особи у відносинах у мережі Інтернет; дізнатися про перспективи запровадження у цивілістичну доктрину концепції цифрової ідентичності як проекції фізичної особи в мережі Інтернет.

Крім того рекомендовано до використання у навчальному процесі наступні публікації:

Монографії:

1. Токарева В.О. Зловживання цивільним правом та право на інформацію. Права приватної особи в умовах пандемії COVID-19: проблеми здійснення і захисту: монографія / Є.О. Харитонов, О.І. Харитонова, К.І. Бєляков; Є.О. Харитонова, О.І. Харитонової, К.Г. Некіт. Одеса: Гельветика, 2020. С. 194-204.

2. Токарева В.О. Обмеження майнових прав інтелектуальної власності у сфері охорони здоров'я // Приватні та публічні інтереси в умовах COVID-19: колізії та правові шляхи вирішення. колективна монографія; за ред. Харитонова Є.О., Харитонова О.І., Булеца С.Б. Одеса 2021. С. 279-293.

3. Токарева В.О. Розвиток цифрової ідентичності як елементу сервісної держави в умовах війни. Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: монографія [Електронне видання] / за ред.: Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт; упор.-укл. Ю. С.

Маршук; НУ «Одеська юридична академія». – Одеса: Фенікс, 2023. – 336 с. С 86-97.– Режим доступу: https://hdl.handle.net/11300/23423

4. Токарева В.О. Віртуальна ідентичність як проекція фізичної особи у мережі Інтернет. The European dimension of modern legal science: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2022. С. 406-418. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/266/7388/15360-1

5. Токарева В.О. Анонімність в мережі Інтернет. Law in the postmodern epoch: general characteristics and manifestation particularities in separate law branches: Scientific monograph. Riga, Latvia: "Baltija Publishing", 2023. 776 p. С.6-1-617. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/299/8343/17405-1

6. Токарева В.О. Інформаційна приватність за законодавством ЄС: виклики та перспективи. Modern paradigm of public and private law amidst sustainable development: Scientific monograph. Vol. 2. Riga, Latvia: Baltija Publishing, 2023. 408 p. С. 295-310. DOI https://doi.org/10.30525/978-9934-26-331-6-32. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/363/9891/20595-1

Наукові статті:

7. Токарева В.О. Наслідки порушення прав інтелектуальної власності китайськими товаровиробниками. *Часопис цивілістики.* 2016. № 20. С. 202-206. URL: http://clj.nuoua.od.ua/archive/20/43.pdf

8. Токарева В.О. Авторське право у цифрову добу. *Часопис цивілістики.* 2017. №26. С. 93-98. URL: http://clj.nuoua.od.ua/archive/26/22.pdf

9. Токарева В.О. Інтелектуальна власність КНР: на шляху інновацій. *Науковий Вісник МГУ.* 2018. № 32. С. 53-56. URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc32/14.pdf

10. Токарева В.О. Щодо питання творчості та штучного інтелекту. *Прикарпатський юридичний вісник.* 2018. № 1(22). С. 55-58. http://pjv.nuoua.od.ua/v1_2018/15.pdf

11. Токарева В.О. Онлайн платформи: виклик авторському праву у цифрову добу. *Часопис цивілістики.* 2018. № 29. С. 107-111. URL: http://clj.nuoua.od.ua/archive/29/23.pdf

12. Токарева В.О. Обчислювальна творчість (щодо питання творчості штучного інтелекту). *Часопис цивілістики.* 2018. № 30. С. 38-43. URL: http://clj.nuoua.od.ua/archive/30/10.pdf

13. Токарева В.О. Щодо питання інформаційної природи авторського права. *Часопис цивілістики.* 2019. № 33. С. 61-66. URL: http://clj.nuoua.od.ua/archive/33/13.pdf

14. Токарева В.О. Умови охороноздатності об'єктів авторського права. *Приватне та публічне право.* 2019. № 3. 39-43. URL: http://www.pp-law.in.ua/archive/3_2019/11.pdf

15. Токарева В.О. Похідні твори у галузі сучасного мистецтва. *Науковий вісник публічного та приватного права.* 2019. № 6. С. 35-40. URL: http://nvppp.in.ua/vip/2019/6/7.pdf

16. Токарева В.О. Сумлінне використання та похідні твори у сучасному мистецтві. *Таврійський національний університет імені В.І. Вернадського.* 2020. № 31 (70). № 2. С. 121-125. URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_1/25.pdf

17. Токарева В.О. Щодо питання захисту прав інтелектуальної власності. *Часопис Цивілістики.* 2020. №. 36. 51-56. URL: http://clj.nuoua.od.ua/archive/36/11.pdf

18. Токарева В.О. Формування категорії «віртуальна ідентичність» у мережі Інтернет. *Часопис Цивілістики.* 2022. № 45. С. 63-67. URL: http://chascyvil.onua.edu.ua/index.php/chc/article/view/468/511

19. Токарева В.О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 3. С. 47-52. URL: http://apnl.dnu.in.ua/3_2022/8.pdf

20. Токарева В.О. Окремі питання реалізації права на видалення. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 4. С. 43-47. URL: http://apnl.dnu.in.ua/4_2022/8.pdf

21. Давидов І.В., Токарева В.О. Захист права на повагу до честі та гідності, ділової репутації, публічних осіб. *Держава та регіони. Серія Право.* 2022. № 1 (75). С. 131-135. URL: http://www.law.stateandregions.zp.ua/archive/1_2022/22.pdf

22. Токарева В.О. Щодо визначення персональних даних в умовах Євроінтеграційних процесів. *Південноукраїнський правничий часопис.* 2022. № 4. Том 3. С.169-174 URL:. http://www.sulj.oduvs.od.ua/archive/2022/4/part_3/28.pdf

23. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Публічне та приватне право.* 2022. № 4. С. 35-40. URL: http://pp-law.in.ua/archive/4_2022/6.pdf

24. Токарева В.О. До питання прийняття рішень із застосування алгоритмів. *Публічне та приватне право.* 2023. № 1. С. 30-35. URL: http://pp-law.in.ua/archive/1_2023/5.pdf

25. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики.* 2023. № 49. С. 32-37. URL: http://clj.nuoua.od.ua/archive/49/5.pdf

26. Токарева В.О. Правове регулювання застосування систем віддаленої біометричної ідентифікації в ЄС. *Публічне та приватне право.* 2023. № 2. С. 3-8. URL: http://pp-law.in.ua/archive/2_2023/1.pdf

27. Токарева В. Реалізація сімейної правоздатності фізичної особи за допомогою мережі Інтернет. *Юридичний бюлетень.* № 29. 2023. С. 134-141. http://www.lawbulletin.oduvs.od.ua/archive/2023/29/14.pdf

28. Токарева В.О. Порушення прав на торговельні марки в мережі Інтернет. Юридичний науковий електронний журнал. 2023. №10. С.141-144. URL: http://www.lsej.org.ua/10_2023/32.pdf

29. Токарева В.О. Окремі питання управління майном фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С.129-131. URL: http://www.lsej.org.ua/8_2024/30.pdf

30. Токарева В.О. До питання права на зображення (голограму) фізичної особи після смерті в умовах поширення технологій ШІ. *Часопис цивілістики.* 2024. № 54. С. 43-48. URL: http://clj.nuoua.od.ua/archive/54/8.pdf

31. Токарева В.О., Личко В.С. Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С. 848 -851. URL: http://www.lsej.org.ua/4_2024/209.pdf

32. Токарева В.О., Личко В.С. Спадкування об'єктів в мережі Інтернет: досвід західних держав. *Часопис цивілістики.* 2024. № 53. С. 41-46. URL: http://clj.nuoua.od.ua/archive/53/9.pdf

33. Давидова І.В., Токарева В.О. Цифрова нерівність і право на доступ до Інтернету. *Юридичний вісник.* 2024. № 6. С. 68-75. URL: http://yurvisnyk.in.ua/v6_2024/10.pdf

34. Токарева В.О. Проблемні питання творчості в умовах цифрової доби. *European political and law discourse.* 2019. №2. С.123-128. URL: https://eppd13.cz/wp-content/uploads/2019/2019-6-2/eppd_2019_6_2.pdf

35. Токарева В.О. Окремі аспекти сирітських творів в умовах інтеграційних процесів. *Jurnaluljuridic.* 2019. № №3. с. 97-101. http://www.jurnaluljuridic.in.ua/archive/2019/3/part_1/22.pdf

36. Токарева В.О. Обчислювальна (Алгоритмічна) творчість: постановка проблеми. *Visegrad Jurnal on Human Rights.* 2019. № 2. (V.2) С. 150-155. https://journal-vjhr.sk/wp-content/uploads/2020/12/Vyshegrad-2_2019_Tom-2.pdf

37. Токарева В.О. Окремі питання легалізації сирітських творів. *Recht der Osteuropäischen Staaten (ReOS).* 2019. №1. С. 197-201.URL: https://www.uni-goettingen.de/de/document/download/ca207b2e626da0c3a651dab3e413069e.pdf/ReOS%2001%20aus%202019.pdf

Голова комісії: _____ Мінас АРАКЕЛЯН

Члени комісії: _____ Галина УЛЬЯНОВА

_____ Людмила КУЗНЕЦОВА

_____ Євген ХИЖНЯК

_____ Євген ХАРИТОНОВ

Додаток В

1

«ЗАТВЕРДЖУЮ»

Ректор
Хмельницького університету
управління та права
імені Леоніда Юзькова, доктор юридичних
наук, професор, заслужений юрист України

Олег ОМЕЛЬЧУК

«20» травня 2025 року

А К Т
про реалізацію результатів наукових досліджень
Токаревої Віри Олександрівни на тему:
«ПРАВОСУБ'ЄКТНІСТЬ ФІЗИЧНОЇ ОСОБИ У ВІДНОСИНАХ У МЕРЕЖІ ІНТЕРНЕТ»

Комісія у складі: голови, декана юридичного факультету, кандидата юридичних наук, доцента Захарчука Віктора Миколайовича, членів комісії: завідувача кафедри приватного права, доктора юридичних наук, професора Гринько Світлани Дмитрівни, доцента кафедри приватного права, кандидата юридичних наук, доцента Якимчук Світлани Олексіївни, стверджує цим актом, що розроблені в ході дисертаційного дослідження Токаревої Віри Олександрівни наукові положення і висновки з теми «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» були детально вивчені колективом кафедри приватного права Хмельницького університету управління та права імені Леоніда Юзькова та реалізовані в освітньому процесі.

Зокрема, дисертанткою було надано комісії для ознайомлення перераховані у дисертації наукові публікації:

1. Токарева В.О. Зловживання цивільним правом та право на інформацію. Права приватної особи в умовах пандемії COVID-19: проблеми здійснення і захисту: монографія / Є.О. Харитонов, О.І. Харитонова, К.І. Бєляков; Є.О. Харитонова, О.І. Харитонової, К.Г. Некіт. Одеса: Гельветика, 2020. С. 194-204.

2. Токарева В.О. Обмеження майнових прав інтелектуальної власності у сфері охорони здоров'я // Приватні та публічні інтереси в умовах COVID-19: колізії та правові шляхи вирішення. колективна монографія; за ред. Харитонова Є.О., Харитонова О.І., Булеца С.Б. Одеса 2021. С. 279-293.

3. Токарева В.О. Розвиток цифрової ідентичності як елементу сервісної держави в умовах війни. Проблеми здійснення та захисту цивільних прав в

умовах воєнного стану: монографія [Електронне видання] / за ред.: Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт; упор.-укл. Ю. С. Маршук; НУ «Одеська юридична академія». – Одеса: Фенікс, 2023. – 336 с. С 86-97.– Режим доступу: https://hdl.handle.net/11300/23423

4. Токарева В.О. Віртуальна ідентичність як проекція фізичної особи у мережі Інтернет. The European dimension of modern legal science: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2022. С. 406-418. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/266/7388/15360-1

5. Токарева В.О. Анонімність в мережі Інтернет. Law in the postmodern epoch: general characteristics and manifestation particularities in separate law branches: Scientific monograph. Riga, Latvia: "Baltija Publishing", 2023. 776 p. С.6-1-617. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/299/8343/17405-1

6. Токарева В.О. Інформаційна приватність за законодавством ЄС: виклики та перспективи. Modern paradigm of public and private law amidst sustainable development: Scientific monograph. Vol. 2. Riga, Latvia: Baltija Publishing, 2023. 408 p. С. 295-310. DOI https://doi.org/10.30525/978-9934-26-331-6-32. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/363/9891/20595-1

7. Токарева В.О. Наслідки порушення прав інтелектуальної власності китайськими товаровиробниками. *Часопис цивілістики.* 2016. № 20. С. 202-206. URL: http://clj.nuoua.od.ua/archive/20/43.pdf

8. Токарева В.О. Авторське право у цифрову добу. *Часопис цивілістики.* 2017. №26. С. 93-98. URL: http://clj.nuoua.od.ua/archive/26/22.pdf

9. Токарева В.О. Інтелектуальна власність КНР: на шляху інновацій. *Науковий Вісник МГУ.* 2018. № 32. С. 53-56. URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc32/14.pdf

10. Токарева В.О. Щодо питання творчості та штучного інтелекту. *Прикарпатський юридичний вісник.* 2018. № 1(22). С. 55-58. http://pjv.nuoua.od.ua/v1_2018/15.pdf

11. Токарева В.О. Онлайн платформи: виклик авторському праву у цифрову добу. *Часопис цивілістики.* 2018. № 29. С. 107-111. URL: http://clj.nuoua.od.ua/archive/29/23.pdf

12. Токарева В.О. Обчислювальна творчість (щодо питання творчості штучного інтелекту). *Часопис цивілістики.* 2018. № 30. С. 38-43. URL: http://clj.nuoua.od.ua/archive/30/10.pdf

13. Токарева В.О. Щодо питання інформаційної природи авторського права. *Часопис цивілістики.* 2019. № 33. С. 61-66. URL: http://clj.nuoua.od.ua/archive/33/13.pdf

14. Токарева В.О. Умови охороноздатності об'єктів авторського права. *Приватне та публічне право.* 2019. № 3. 39-43. URL: http://www.pp-law.in.ua/archive/3_2019/11.pdf

15. Токарева В.О. Похідні твори у галузі сучасного мистецтва. *Науковий вісник публічного та приватного права.* 2019. № 6. С. 35-40. URL: http://nvppp.in.ua/vip/2019/6/7.pdf

16. Токарева В.О. Сумлінне використання та похідні твори у сучасному мистецтві. *Таврійський національний університет імені В.І. Вернадського.* 2020. № 31 (70). № 2. С. 121-125. URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_1/25.pdf

17. Токарева В.О. Щодо питання захисту прав інтелектуальної власності. *Часопис Цивілістики.* 2020. №. 36. 51-56. URL: http://clj.nuoua.od.ua/archive/36/11.pdf

18. Токарева В.О. Формування категорії «віртуальна ідентичність» у мережі Інтернет. *Часопис Цивілістики.* 2022. № 45. С. 63-67. URL: http://chascyvil.onua.edu.ua/index.php/chc/article/view/468/511

19. Токарева В.О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 3. С. 47-52. URL: http://apnl.dnu.in.ua/3_2022/8.pdf

20. Токарева В.О. Окремі питання реалізації права на видалення. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 4. С. 43-47. URL: http://apnl.dnu.in.ua/4_2022/8.pdf

21. Давидов І.В., Токарева В.О. Захист права на повагу до честі та гідності, ділової репутації, публічних осіб. *Держава та регіони. Серія Право.* 2022. № 1 (75). С. 131-135. URL: http://www.law.stateandregions.zp.ua/archive/1_2022/22.pdf

22. Токарева В.О. Щодо визначення персональних даних в умовах Євроінтеграційних процесів. *Південноукраїнський правничий часопис.* 2022. № 4. Том 3. С.169-174 URL:. http://www.sulj.oduvs.od.ua/archive/2022/4/part_3/28.pdf

23. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Публічне та приватне право.* 2022. № 4. С. 35-40. URL: http://pp-law.in.ua/archive/4_2022/6.pdf

24. Токарева В.О. До питання прийняття рішень із застосування алгоритмів. *Публічне та приватне право.* 2023. № 1. С. 30-35. URL: http://pp-law.in.ua/archive/1_2023/5.pdf

25. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики.* 2023. № 49. С. 32-37. URL: http://clj.nuoua.od.ua/archive/49/5.pdf

26. Токарева В.О. Правове регулювання застосування систем віддаленої біометричної ідентифікації в ЄС. *Публічне та приватне право*. 2023. № 2. С. 3-8. URL: http://pp-law.in.ua/archive/2_2023/1.pdf

27. Токарева В. Реалізація сімейної правоздатності фізичної особи за допомогою мережі Інтернет. *Юридичний бюлетень*. № 29. 2023. С. 134-141. http://www.lawbulletin.oduvs.od.ua/archive/2023/29/14.pdf

28. Токарева В.О. Порушення прав на торговельні марки в мережі Інтернет. Юридичний науковий електронний журнал. 2023. №10. С.141-144. URL: http://www.lsej.org.ua/10_2023/32.pdf

29. Токарева В.О. Окремі питання управління майном фізичної особи. *Юридичний науковий електронний журнал*. 2024. № 4. С.129-131. URL: http://www.lsej.org.ua/8_2024/30.pdf

30. Токарева В.О. До питання права на зображення (голограму) фізичної особи після смерті в умовах поширення технологій ШІ. *Часопис цивілістики*. 2024. № 54. С. 43-48. URL: http://clj.nuoua.od.ua/archive/54/8.pdf

31. Токарева В.О., Личко В.С. Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал*. 2024. № 4. С. 848 -851. URL: http://www.lsej.org.ua/4_2024/209.pdf

32. Токарева В.О., Личко В.С. Спадкування об'єктів в мережі Інтернет: досвід західних держав. *Часопис цивілістики*. 2024. № 53. С. 41-46. URL: http://clj.nuoua.od.ua/archive/53/9.pdf

33. Давидова І.В., Токарева В.О. Цифрова нерівність і право на доступ до Інтернету. *Юридичний вісник*. 2024. № 6. С. 68-75. URL: http://yurvisnyk.in.ua/v6_2024/10.pdf

34. Токарева В.О. Проблемні питання творчості в умовах цифрової доби. *European political and law discourse*. 2019. №2. С.123-128. URL: https://eppd13.cz/wp-content/uploads/2019/2019-6-2/eppd_2019_6_2.pdf

35. Токарева В.О. Окремі аспекти сирітських творів в умовах інтеграційних процесів. *Jurnaluljuridic*. 2019. № №3. с. 97-101. http://www.jurnaluljuridic.in.ua/archive/2019/3/part_1/22.pdf

36. Токарева В.О. Обчислювальна (Алгоритмічна) творчість: постановка проблеми. *Visegrad Jurnal on Human Rights*. 2019. № 2. (V.2) С. 150-155. https://journal-vjhr.sk/wp-content/uploads/2020/12/Vyshegrad-2_2019_Tom-2.pdf

37. Токарева В.О. Окремі питання легалізації сирітських творів. *Recht der Osteuropäischen Staaten (ReOS)*. 2019. №1. С. 197-201.URL: https://www.uni-goettingen.de/de/document/download/ca207b2c626da0c3a651dab3e413069e.pdf/ReOS%2001%20aus%202019.pdf

38. Nekit K., Tokareva V., Zubar V. (2020). Artificial intelligence as a potential subject of property and intellectual property relations. Ius Humani. Law Journal, 9 (1), 231-250. https://doi.org/https://doi.org/10.31207/ih.v9i1.227

39. Tokareva V. Davydova I., Adamova E. Legal problems of the use of orphan works in digital age. Juridical Tribune. 2021. № 11. P. 453-471. http://www.tribunajuridica.eu/arhiva/An11v3/3.%20Tokareva%20Davydova%20Adamova.pdf

40. Tokareva V. Digital identity as the element of concept of service-oriented state. Doctrina et Usu in Business Law // Contributions to the 12th International Conference Challenges of Business Law in the Third Millennium, November 25, 2022, Bucharest ADJURIS. P. 281-301.

41. Токарева В.О. Проблемні аспекти творчості в епоху цифрових трансформацій // Взаємодія громадянського суспільства, особи і держави: вектор удосконалення: Міжнародна науково-практична конференція. (м. Київ, 22 червня 2021) Київський регіональний центр НАПрН, 2021. С. 179-182.

42. Токарева В.О. Проблеми легалізації сирітських творів в умовах інформаційного суспільства // «Проблеми та стан дотримання і захисту прав людини в Україні»: Матеріали міжнародної науково-практичної конференції, м. Львів, 20–21 серпня 2021 р. – Львів: Західноукраїнська організація «Центр правничих ініціатив», С. 31-34.

43. Токарева В.О. Окремі питання реалізації права на творчість особами засудженими до позбавлення волі // Юридична наука: виклики і сьогодення: матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 11–12 червня 2021 р.). – Одеса : ГО «Причорноморська фундація права», 2021. С. 49-52.

44. Токарева В.О. Еволюція концепту творчості та розвитку інновацій в КНР // Сучасне правотворення: питання теорії та практики: Матеріали міжнародної науково-практичної конференції, м. Дніпро, 4–5 червня 2021 р. – Дніпро: ГО «Правовий світ», 2021. С. 51-54.

45. Токарева В.О. До питання результатів інтелектуальної діяльності та штучного інтелекту // Особливості розвитку законодавства України у контексті євроінтеграційних процесів: міжнародна науково-практична конференція, м. Харків, 4–5 червня 2021 р. – Харків : Східно- українська наукова юридична організація, 2021. – С. 68-71.

46. Токарева В.О. Право на свободу вираження творчості // Актуальні питання реформування правової системи України: Матеріали міжнародної науково-практичної конференції, м. Дніпро, 2–3 липня 2021 р. – Дніпро: ГО «Правовий світ», 2021. – С. 17-20.

47. Токарева В.О. Результати творчості сгенеровані штучним інтелектом // Сучасний вимір держави і права: матеріали міжнародної науково-практичної конференції, м. Львів, 18–19 червня 2021 р. – Львів: Західноукраїнська організація «Центр правничих ініціатив», 2021. – С. 102-106.

48. Токарева В.О. Право на видалення та право на чистий цифровий лист // Правове регулювання суспільних відносин: перспективні напрями на шляху

до сталого розвитку : матеріали Міжнародної науково- практичної конференції, 28–29 жовтня 2022 р., м. Київ. – Львів – Торунь : Liha-Pres, 2022. – С. 46-50.

49. Токарева В.О. Щодо питання цифрової ідентичності в умовах війни. Приватне право в умовах війни: матеріали всеукр. наук. конф. (Одеса, 15 листоп. 2022 р.) / за заг. ред.: д.ю.н., проф. Є. Харитонова, д.ю.н., проф. І. Давидової ; НУ «Одеська юридична академія. – Одеса, 2022. – 1004 с. С. 111-116. URL: https://hdl.handle.net/11300/25131

50. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. Становлення та розвиток правової держави: проблеми теорії та практики: Матеріали XV міжнародної науково-практичної конференції, що присвячена 102-річчю Національного університету кораблебудування імені адмірала Макарова, м. Миколаїв. 28–29 грудня 2022 р. Львів – Торунь: Liha-Pres, 2022. – 504 с. С. 351-364.

51. Токарева В.О. Деякі питання щодо категорії «віртуальна ідентичність» у мережі Інтернет Integration of Education, Science and Business in Modern Environment: Summer Debates: Proceedings of the 4th International Scientific and Practical Internet Conference, August 15-16, 2022. FOP Marenichenko V.V., Dnipro, Ukraine, 82 p. С. 67-69.

Наведені наукові публікації були розглянуті науково-педагогічними працівниками кафедри приватного права Хмельницького університету управління та права імені Леоніда Юзькова та були включені до матеріалів лекційних занять з таких навчальних дисциплін: «Цивільне право», «Право інтелектуальної власності», «Цивільно-правовий захист особистих немайнових прав».

Голова комісії:
декан юридичного факультету,
кандидат юридичних наук, доцент Віктор ЗАХАРЧУК

Члени комісії:
завідувач кафедри
приватного права,
доктор юридичних наук, професор Світлана ГРИНЬКО

доцент кафедри
приватного права,
кандидат юридичних наук, доцент Світлана ЯКИМЧУК

Додаток Г

ЗАТВЕРДЖУЮ
Перший проректор
Одеського державного
університету внутрішніх справ
полковник поліції

Максим КОРНІЄНКО
«09» 05 2025 р.

АКТ
впровадження наукових розробок дисертаційного дослідження Токаревої В.О. на тему «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» до освітнього процесу Одеського державного університету внутрішніх справ

м. Одеса 09.05. 2025 р.

Комісія у складі:

1) начальника відділу організації освітнього процесу, полковника поліції Сіфорова О.І.;

2) завідувача кафедри цивільно-правових дисциплін інституту права та безпеки, кандидата юридичних наук, професора Маковія В.П.;

3) професора кафедри державно-правових дисциплін інституту права та безпеки, кандидата політичних наук, доцента Юрченка М.М.

склала цей акт з приводу того, що Токаревою Вірою Олександрівною виконані результати дисертаційного дослідження на тему: «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» підготовленого на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.03 – цивільне право і цивільний процес; сімейне право; міжнародне приватне право, у вигляді циклу наукових публікацій:

1. Токарева В.О. Розвиток цифрової ідентичності як елементу сервісної держави в умовах війни. Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: монографія [Електронне видання] / за ред.: Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт; упор.-укл. Ю. С. Маршук; НУ «Одеська юридична академія». Одеса: Фенікс, 2023. 336 с. С 86-97.

2. Токарева В.О. Анонімність в мережі Інтернет. Law in the postmodern epoch: general characteristics and manifestation particularities in separate law branches: Scientific monograph. Riga, Latvia: "Baltija Publishing", 2023. 776 p. C.6-1-617.

3. Токарева В.О. Інформаційна приватність за законодавством ЄС: виклики та перспективи. Modern paradigm of public and private law amidst

sustainable development: Scientific monograph. Vol. 2. Riga, Latvia: Baltija Publishing, 2023. 408 p. С. 295-310.

4. Токарева В.О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 3. С. 47-52.

5. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики.* 2023. № 49. С. 32-37.

6. Токарева В.О. Правове регулювання застосування систем віддаленої біометричної ідентифікації в ЄС. *Публічне та приватне право.* 2023. № 2. С. 3-8.

7. Токарева В.О. Порушення прав на торговельні марки в мережі Інтернет. Юридичний науковий електронний журнал. 2023. №10. С.141-144.

8. Токарева В.О. До питання права на зображення (голограму) фізичної особи після смерті в умовах поширення технологій ШІ. *Часопис цивілістики.* 2024. № 54. С. 43-48.

9. Токарева В.О., Личко В.С. Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С. 848 -851.

10. Токарева В.О., Личко В.С. Спадкування об'єктів в мережі Інтернет: досвід західних держав. *Часопис цивілістики.* 2024. № 53. С. 41-46.

11. Давидова І.В., Токарева В.О. Цифрова нерівність і право на доступ до Інтернету. *Юридичний вісник.* 2024. № 6. С. 68-75.

Комісією вивчені пропозиції і рекомендації щодо впровадження циклу наукових публікацій Токаревої Віри Олександрівною за результатами дисертаційного дослідження на тему: «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» підготовленого на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.03 – цивільне право і цивільний процес; сімейне право; міжнародне приватне право в освітній процес Одеського державного університету внутрішніх справ.

Комісія дійшла висновку, що зазначені положення віднайшли відображення в освітньому процесі Одеського державного університету внутрішніх справ, зокрема:

- в навчально-методичних матеріалах освітньої компоненти «Актуальні проблеми права інтелектуальної власності» освітньої (професійної) програми «Право» другого (магістерського) рівня вищої освіти за спеціальністю 081 «Право» (методичні рекомендації для проведення практичних занять та самостійної роботи, матеріали методичного супроводження дистанційного навчання на порталі МІА: Освіта) та використані при проведені семінарських та практичних занять.

- в навчально-методичних матеріалах освітньої компоненти «Приватне право: практика тлумачення і застосування» освітньої (професійної) програми «Право» другого (магістерського) рівня вищої освіти за спеціальністю 081 «Право» (методичні рекомендації для проведення практичних занять та самостійної роботи, матеріали методичного супроводження дистанційного навчання на порталі МІА: Освіта) та використані при проведені семінарських та практичних занять.

Члени комісії:

Начальник відділу
організації освітнього процесу,
полковник поліції — Олександр СІФОРОВ

Завідувач кафедри
цивільно-правових дисциплін
інституту права та безпеки,
кандидат юридичних наук, професор — Віктор МАКОВІЙ

Професор кафедри
державно-правових дисциплін
інституту права та безпеки,
кандидат політичних наук, доцент — Микола ЮРЧЕНКО

Додаток Ґ

«ЗАТВЕРДЖУЮ»
голова Київського районного суду
м. Одеси
_____ С.А. Чванкін
«___» _____ 2025 р.

АКТ
про впровадження результатів дисертаційного дослідження
В.О. Токаревої на тему: «Правосуб'єктність
фізичної особи у відносинах у мережі Інтернет»
у практичну діяльність Київського районного суду м. Одеси

Комісія у складі:
заступника голови Київського районного суду м. Одеси Петренка В.С.,
судді Київського районного суду м. Одеси Калініченко Л.В.,
судді Київського районного суду м. Одеси Скриль Ю.А.,
склала цей акт з приводу того, що комісією розглянуто результати наукових розробок в межах дисертаційного дослідження В.О. Токаревої на тему «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» у вигляді наукових публікацій, які присвячені комплексному аналізу категорії правосуб'єктності фізичної особи у відносинах в мережі Інтернет та розвитку автоматизованих систем під час прийняття юридично значущих рішень.

Комісія вважає, що викладені у публікаціях окремі пропозиції та висновки заслуговують практичного використання у діяльності Київського районного суду м. Одеси.

Рекомендовано до ознайомлення та використання в практичній діяльності суддями наступні публікації:

Монографії:

1. Токарева В.О. Зловживання цивільним правом та право на інформацію. Права приватної особи в умовах пандемії COVID-19: проблеми здійснення і захисту: монографія / Є.О. Харитонов, О.І. Харитонова, К.І. Бєляков; Є.О. Харитонова, О.І. Харитонової, К.Г. Некіт. Одеса: Гельветика, 2020. С. 194-204.
2. Токарева В.О. Обмеження майнових прав інтелектуальної власності у сфері охорони здоров'я // Приватні та публічні інтереси в умовах COVID-19: колізії та правові шляхи вирішення. колективна монографія; за ред. Харитонова Є.О., Харитонова О.І., Булеца С.Б. Одеса 2021. С. 279-293.

3. Токарева В.О. Розвиток цифрової ідентичності як елементу сервісної держави в умовах війни. Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: монографія [Електронне видання] / за ред.: Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт; упор.-укл. Ю. С. Маршук; НУ «Одеська юридична академія». – Одеса: Фенікс, 2023. – 336 с. С 86-97.

4. Токарева В.О. Віртуальна ідентичність як проекція фізичної особи у мережі Інтернет. The European dimension of modern legal science: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2022. С. 406-418.

5. Токарева В.О. Анонімність в мережі Інтернет. Law in the postmodern epoch: general characteristics and manifestation particularities in separate law branches: Scientific monograph. Riga, Latvia: "Baltija Publishing", 2023. 776 p. С.6-1-617.

6. Токарева В.О. Інформаційна приватність за законодавством ЄС: виклики та перспективи. Modern paradigm of public and private law amidst sustainable development: Scientific monograph. Vol. 2. Riga, Latvia: Baltija Publishing, 2023. 408 p. С. 295-310.

Наукові статті у фахових виданнях:

7. Токарева В.О. Наслідки порушення прав інтелектуальної власності китайськими товаровиробниками. *Часопис цивілістики.* 2016. № 20. С. 202-206.

8. Токарева В.О. Авторське право у цифрову добу. *Часопис цивілістики.* 2017. №26. С. 93-98.

9. Токарева В.О. Інтелектуальна власність КНР: на шляху інновацій. *Науковий Вісник МГУ.* 2018. № 32. С. 53-56.

10. Токарева В.О. Щодо питання творчості та штучного інтелекту. *Прикарпатський юридичний вісник.* 2018. № 1(22). С. 55-58.

11. Токарева В.О. Онлайн платформи: виклик авторському праву у цифрову добу. *Часопис цивілістики.* 2018. № 29. С. 107-111.

12. Токарева В.О. Обчислювальна творчість (щодо питання творчості штучного інтелекту). *Часопис цивілістики.* 2018. № 30. С. 38-43.

13. Токарева В.О. Щодо питання інформаційної природи авторського права. *Часопис цивілістики.* 2019. № 33. С. 61-66.

14. Токарева В.О. Умови охороноздатності об'єктів авторського права. *Приватне та публічне право.* 2019. № 3. 39-43.

15. Токарева В.О. Похідні твори у галузі сучасного мистецтва. *Науковий вісник публічного та приватного права.* 2019. № 6. С. 35-40.

16. Токарева В.О. Сумлінне використання та похідні твори у сучасному мистецтві. *Таврійський національний університет імені В.І. Вернадського.* 2020. № 31 (70). № 2. С. 121-125.

17. Токарева В.О. Щодо питання захисту прав інтелектуальної власності. *Часопис Цивілістики.* 2020. №. 36. 51-56.

18. Токарева В.О. Формування категорії «віртуальна ідентичність» у мережі Інтернет. *Часопис Цивілістики.* 2022. № 45. С. 63-67. URL: http://chascyvil.onua.edu.ua/index.php/chc/article/view/468/511

19. Токарева В.О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 3. С. 47-52. URL: http://apnl.dnu.in.ua/3_2022/8.pdf

20. Токарева В.О. Окремі питання реалізації права на видалення. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 4. С. 43-47. URL: http://apnl.dnu.in.ua/4_2022/8.pdf

21. Давидов І.В., Токарева В.О. Захист права на повагу до честі та гідності, ділової репутації, публічних осіб. *Держава та регіони. Серія Право.* 2022. № 1 (75). С. 131-135. URL: http://www.law.stateandregions.zp.ua/archive/1_2022/22.pdf

22. Токарева В.О. Щодо визначення персональних даних в умовах Євроінтеграційних процесів. *Південноукраїнський правничий часопис.* 2022. № 4. Том 3. С.169-174 URL:. http://www.sulj.oduvs.od.ua/archive/2022/4/part_3/28.pdf

23. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Публічне та приватне право.* 2022. № 4. С. 35–40. URL: http://pp-law.in.ua/archive/4_2022/6.pdf

24. Токарева В.О. До питання прийняття рішень із застосування алгоритмів. *Публічне та приватне право.* 2023. № 1. С. 30-35. URL: http://pp-law.in.ua/archive/1_2023/5.pdf

25. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики.* 2023. № 49. С. 32-37. URL: http://clj.nuoua.od.ua/archive/49/5.pdf

26. Токарева В.О. Правове регулювання застосування систем віддаленої біометричної ідентифікації в СС. *Публічне та приватне право.* 2023. № 2. С. 3-8. URL: http://pp-law.in.ua/archive/2_2023/1.pdf

27. Токарева В. Реалізація сімейної правоздатності фізичної особи за допомогою мережі Інтернет. *Юридичний бюлетень.* № 29. 2023. С. 134-141. http://www.lawbulletin.oduvs.od.ua/archive/2023/29/14.pdf

28. Токарева В.О. Порушення прав на торговельні марки в мережі Інтернет. Юридичний науковий електронний журнал. 2023. №10. С.141-144. URL: http://www.lsej.org.ua/10_2023/32.pdf

29. Токарева В.О. Окремі питання управління майном фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С.129-131. URL: http://www.lsej.org.ua/8_2024/30.pdf

30. Токарева В.О. До питання права на зображення (голограму) фізичної особи після смерті в умовах поширення технологій ШІ. *Часопис цивілістики.* 2024. № 54. С. 43-48. URL: http://clj.nuoua.od.ua/archive/54/8.pdf

31. Токарева В.О., Личко В.С. Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С. 848 -851. URL: http://www.lsej.org.ua/4_2024/209.pdf

32. Токарева В.О., Личко В.С. Спадкування об'єктів в мережі Інтернет: досвід західних держав. *Часопис цивілістики.* 2024. № 53. С. 41-46. URL: http://clj.nuoua.od.ua/archive/53/9.pdf

33. Давидова І.В., Токарева В.О. Цифрова нерівність і право на доступ до Інтернету. *Юридичний вісник.* 2024. № 6. С. 68-75.

Заступник голови
Київського районного суду м. Одеси Петренко В.С.

Суддя
Київського районного суду м. Одеси Калініченко Л.В.

Суддя
Київського районного суду м. Одеси Скриль Ю.А.

Додаток Д

ЗАТВЕРДЖУЮ»
Заступник начальника Південного
міжрегіонального управління
Міністерства юстиції (м. Одеса)

_____ А.М. Буряченко

«23» квітня 2025 року

АКТ
про впровадження результатів дисертаційного дослідження
Токаревої Віри Олександрівни
на тему
«Правосуб'єктність фізичної особи у відносинах у мережі Інтернет»
в практичну діяльність Південного міжрегіонального управління
Міністерства юстиції (м. Одеса)

Комісія у складі: заступника начальника Південного міжрегіонального управління Міністерства юстиції (м. Одеса) А.М. Буряченко, начальника відділу організації роботи та розвитку персоналу в Одеській області Управління персоналу Південного міжрегіонального управління Міністерства юстиції (м. Одеса) І.М. Чумак, заступника начальника Управління – начальника відділу судової роботи та міжнародної правової допомоги в Одеській області Управління судової роботи та міжнародної правової допомоги Південного міжрегіонального управління Міністерства юстиції (м. Одеса) К.В. Гуртової, склала цей акт з приводу того, що результати дисертаційного дослідження Токаревої Віри Олександрівни на тему «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» рекомендуються до використання в практичній діяльності Південного міжрегіонального управління Міністерства юстиції (м. Одеса).

Комісією розглянуто результати наукових розробок в межах виконання дисертаційного дослідження «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» у вигляді наукових публікацій, присвячених проблемам реалізації та захисту права фізичної особи в мережі Інтернет.

Комісія вважає, що викладені у публікаціях пропозиції та висновки заслуговують практичного використання у діяльності Південного міжрегіонального управління Міністерства юстиції (м. Одеса). Рекомендовано до використання наступні публікації:

1. Токарева В.О. Зловживання цивільним правом та право на інформацію. Права приватної особи в умовах пандемії COVID-19: проблеми здійснення і захисту: монографія / Є.О. Харитонов, О.І. Харитонова, К.І.

Бєляков; Є.О. Харитонова, О.І. Харитонової, К.Г. Некіт. Одеса: Гельветика, 2020. С. 194-204.

2. Токарева В.О. Обмеження майнових прав інтелектуальної власності у сфері охорони здоров'я // Приватні та публічні інтереси в умовах COVID-19: колізії та правові шляхи вирішення. колективна монографія; за ред. Харитонова Є.О., Харитонова О.І., Булеца С.Б. Одеса 2021. С. 279-293.

3. Токарева В.О. Розвиток цифрової ідентичності як елементу сервісної держави в умовах війни. Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: монографія [Електронне видання] / за ред.: Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт; упор.-укл. Ю. С. Маршук; НУ «Одеська юридична академія». – Одеса: Фенікс, 2023. – 336 с. С 86-97.

4. Токарева В.О. Віртуальна ідентичність як проекція фізичної особи у мережі Інтернет. The European dimension of modern legal science: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2022. С. 406-418.

5. Токарева В.О. Анонімність в мережі Інтернет. Law in the postmodern epoch: general characteristics and manifestation particularities in separate law branches: Scientific monograph. Riga, Latvia: "Baltija Publishing", 2023. 776 p. С.6-1-617.

6. Токарева В.О. Інформаційна приватність за законодавством ЄС: виклики та перспективи. Modern paradigm of public and private law amidst sustainable development: Scientific monograph. Vol. 2. Riga, Latvia: Baltija Publishing, 2023. 408 p. С. 295-310. DOI https://doi.org/10.30525/978-9934-26-331-6-32.

7. Токарева В.О. Щодо питання інформаційної природи авторського права. *Часопис цивілістики.* 2019. № 33. С. 61-66. URL: http://clj.nuoua.od.ua/archive/33/13.pdf

8. Токарева В.О. Умови охороноздатності об'єктів авторського права. *Приватне та публічне право.* 2019. № 3. 39-43. URL: http://www.pp-law.in.ua/archive/3_2019/11.pdf

9. Токарева В.О. Похідні твори у галузі сучасного мистецтва. *Науковий вісник публічного та приватного права.* 2019. № 6. С. 35-40. URL: http://nvppp.in.ua/vip/2019/6/7.pdf

10. Токарева В.О. Сумлінне використання та похідні твори у сучасному мистецтві. *Таврійський національний університет імені В.І. Вернадського.* 2020. № 31 (70). № 2. С. 121-125. URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_1/25.pdf

11. Токарева В.О. Щодо питання захисту прав інтелектуальної власності. *Часопис Цивілістики.* 2020. №. 36. 51-56. URL: http://clj.nuoua.od.ua/archive/36/11.pdf

12. Токарева В.О. Формування категорії «віртуальна ідентичність» у мережі Інтернет. *Часопис Цивілістики.* 2022. № 45. С. 63-67. URL: http://chascyvil.onua.edu.ua/index.php/chc/article/view/468/511

13. Токарева В.О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні*

проблеми вітчизняної юриспруденції. 2022. № 3. С. 47-52. URL: http://apnl.dnu.in.ua/3_2022/8.pdf

14. Токарева В.О. Окремі питання реалізації права на видалення. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 4. С. 43-47. URL: http://apnl.dnu.in.ua/4_2022/8.pdf

15. Давидов І.В., Токарева В.О. Захист права на повагу до честі та гідності, ділової репутації, публічних осіб. *Держава та регіони. Серія Право.* 2022. № 1 (75). С. 131-135. URL: http://www.law.stateandregions.zp.ua/archive/1_2022/22.pdf

16. Токарева В.О. Щодо визначення персональних даних в умовах Євроінтеграційних процесів. *Південноукраїнський правничий часопис.* 2022. № 4. Том 3. С.169-174 URL:. http://www.sulj.oduvs.od.ua/archive/2022/4/part_3/28.pdf

17. Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Публічне та приватне право.* 2022. № 4. С. 35-40. URL: http://pp-law.in.ua/archive/4_2022/6.pdf

18. Токарева В.О. До питання прийняття рішень із застосування алгоритмів. *Публічне та приватне право.* 2023. № 1. С. 30-35. URL: http://pp-law.in.ua/archive/1_2023/5.pdf

19. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики.* 2023. № 49. С. 32-37. URL: http://clj.nuoua.od.ua/archive/49/5.pdf

20. Токарева В.О. Правове регулювання застосування систем віддаленої біометричної ідентифікації в ЄС. *Публічне та приватне право.* 2023. № 2. С. 3-8. URL: http://pp-law.in.ua/archive/2_2023/1.pdf

21. Токарева В. Реалізація сімейної правоздатності фізичної особи за допомогою мережі Інтернет. *Юридичний бюлетень.* № 29. 2023. С. 134-141. http://www.lawbulletin.oduvs.od.ua/archive/2023/29/14.pdf

22. Токарева В.О. Порушення прав на торговельні марки в мережі Інтернет. Юридичний науковий електронний журнал. 2023. №10. С.141-144. URL: http://www.lsej.org.ua/10_2023/32.pdf

23. Токарева В.О. Окремі питання управління майном фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С.129-131. URL: http://www.lsej.org.ua/8_2024/30.pdf

24. Токарева В.О. До питання права на зображення (голограму) фізичної особи після смерті в умовах поширення технологій ШІ. *Часопис цивілістики.* 2024. № 54. С. 43-48. URL: http://clj.nuoua.od.ua/archive/54/8.pdf

25. Токарева В.О., Личко В.С. Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал.* 2024. № 4. С. 848 -851. URL: http://www.lsej.org.ua/4_2024/209.pdf

26. Токарева В.О., Личко В.С. Спадкування об'єктів в мережі Інтернет: досвід західних держав. *Часопис цивілістики.* 2024. № 53. С. 41-46. URL: http://clj.nuoua.od.ua/archive/53/9.pdf

27. Давидова І.В., Токарева В.О. Цифрова нерівність і право на доступ до Інтернету. *Юридичний вісник.* 2024. № 6. С. 68-75. URL: http://yurvisnyk.in.ua/v6_2024/10.pdf

28. Токарева В.О. Проблемні питання творчості в умовах цифрової доби. *European political and law discourse.* 2019. №2. С.123-128. URL: https://eppd13.cz/wp-content/uploads/2019/2019-6-2/eppd_2019_6_2.pdf

29. Токарева В.О. Окремі аспекти сирітських творів в умовах інтеграційних процесів. *Jurnaluljuridic.* 2019. № №3. с. 97-101. http://www.jurnaluljuridic.in.ua/archive/2019/3/part_1/22.pdf

30. Токарева В.О. Обчислювальна (Алгоритмічна) творчість: постановка проблеми. *Visegrad Jurnal on Human Rights.* 2019. № 2. (V.2) С. 150-155. https://journal-vjhr.sk/wp-content/uploads/2020/12/Vyshegrad-2_2019_Tom-2.pdf

Заступник начальника
Південного міжрегіонального управління
Міністерства постиції (м. Одеса) А.М. Буряченко

Начальник відділу організації роботи
та розвитку персоналу в Одеській області
Управління персоналу Південного
міжрегіонального управління
Міністерства юстиції (м. Одеса) І.М. Чумак

Заступник начальника Управління – начальник
відділу судової роботи та міжнародної правової
допомоги в Одеській області Управління
судової роботи та міжнародної правової
допомоги Південного міжрегіонального управління
Міністерства юстиції (м. Одеса) К.В. Гуртова

Додаток Е

Про використання матеріалів
дисертаційного дослідження Токаревої В.О. на тему:
«Правосуб'єктність фізичної особи у відносинах у мережі Інтернет»
на здобуття наукового ступеня доктора юридичних наук

Впровадження концепції «сервісної держави» та автоматизованих систем прийняття рішень передбачає глобальну трансформацію державного управління суспільством, від традиційної бюрократичної системи до управління із застосуванням інформаційно комунікативних технологій. Тож в умовах автоматизації процесів, посилення мережевої структури суспільства, використання аналітики великих даних та програм штучного інтелекту актуалізується питання розуміння та переосмислення правосуб'єктності фізичної особи в мережі Інтернет.

Вищезазначені цифрові трансформації неминуче справляють вплив на впровадження автоматизації процесів які дозволяють забезпечити ефективність прийняття управлінських рішень, реалізації судочинства та виконання судових рішень.

Інтерес становлять положення дисертації щодо перспектив впровадження та використання автоматизованих систем у державному управлінні та судочинстві. Актуальність обумовлюється процесами технологізації та цифровізації судочинства, електронних реєстрів, автоматизацією процесів прийняття юридично значущих рішень, зростанням обсягів збору та обробки даних та поширенням технологій цифрового профайлу фізичної особи.

З одного боку використання автоматизованих систем покликано полегшити процес збору та обробки даних, сприяти ефективності в сферах державного управління, судочинства, розробці стратегій мирного врегулювання конфліктів, з іншого боку ставить виклики пов'язані слабкою прозорістю приймаємих рішень, ризиками упереджень та необхідністю забезпечення прав людини в умовах цифровізації суспільства.

Не менш актуальним є положення дисертації щодо концепції об'єднання профайлів та даних фізичної особи з приватних та державних платформ та реєстрів у єдину цифрову ідентичність, яка є одними провідних елементів «сервісної держави». Крім того заслуговує на увагу положення дисертаційного дослідження щодо використання автоматизованих систем в сфері державного управління, з метою врегулювання конфліктів та примусового виконання судових та інших рішень.

Враховуючи актуальність зазначених питань, наукове дослідження Токаревої В.О. на тему: «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» є актуальним та становить інтерес для практичних працівників, які стикаються з питаннями реалізації правосуб'єктності фізичної особи у відносинах в мережі Інтернет та в умовах автоматизації процесів в сфері державного управління, посередництва, підтримка переговорів та виконання прийнятих рішень.

Звернення до аналізу зазначених питань, зокрема є актуальним, вчасним та може мати практичну цінність, в тому числі в практичній діяльності приватних виконавців Одеської області.

Голова Ради приватних
виконавців Одеської області — В.А. Крецул

12. травня 2025 р.

Додаток Є

АКТ

про впровадження наукових розробок докторської дисертації Токаревої Віри Олександрівни на тему: «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» в практичну діяльність приватного нотаріуса Одеського міського нотаріального округу

Я, приватний нотаріус Одеського міського нотаріального округу Тетяна Дімітрова склала цей акт з приводу того, що результати докторської дисертації Токаревої Віри Олександрівни на тему «Правосуб'єктність фізичної особи у відносинах у мережі Інтернет» за спеціальністю 12.00.03 – «цивільне право і цивільний процес; сімейне право; міжнародне приватне право» використовуються мною у практичній діяльності.

Вважаю, що викладені у публікаціях пропозиції та висновки заслуговують практичного використання у роботі нотаріусів. Рекомендовано до використання наступні публікації:

1. Токарева В.О. Розвиток цифрової ідентичності як елементу сервісної держави в умовах війни. Проблеми здійснення та захисту цивільних прав в умовах воєнного стану: монографія [Електронне видання] / за ред.: Є. О. Харитонова, О. І. Харитонової, К. Г. Некіт; упор.-укл. Ю. С. Маршук; НУ «Одеська юридична академія». – Одеса: Фенікс, 2023. – 336 с. С 86-97.

2. Токарева В.О. Віртуальна ідентичність як проекція фізичної особи у мережі Інтернет. The European dimension of modern legal science: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2022. С. 406-418.

3. Токарева В.О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 3. С. 47-52.

4. Токарева В.О. Щодо визначення персональних даних в умовах Євроінтеграційних процесів. *Південноукраїнський правничий часопис*. 2022. № 4. Том 3. С.169-174 Токарева В.О. Щодо питання цифрової ідентичності у мережі Інтернет. *Публічне та приватне право*. 2022. № 4. С. 35-40.

5. Токарева В.О. До питання прийняття рішень із застосування алгоритмів. *Публічне та приватне право*. 2023. № 1. С. 30-35.

6. Токарева В.О. Правове регулювання використання алгоритмів для прийняття юридично значущих рішень. *Часопис цивілістики*. 2023. № 49. С. 32-37.

7. Токарева В.О. Правове регулювання застосування систем віддаленої біометричної ідентифікації в ЄС. *Публічне та приватне право*. 2023. № 2. С. 3-8. URL: http://pp-law.in.ua/archive/2_2023/1.pdf

8. Токарева В. Реалізація сімейної правоздатності фізичної особи за допомогою мережі Інтернет. *Юридичний бюлетень*. № 29. 2023. С. 134-141.

9. Токарева В.О. Окремі питання управління майном фізичної особи. *Юридичний науковий електронний журнал*. 2024. № 4. С.129-131.

10. Токарева В.О., Личко В.С. Довірче управління майном в мережі Інтернет після смерті фізичної особи. *Юридичний науковий електронний журнал*. 2024. № 4. С. 848 -851. URL: http://www.lsej.org.ua/4_2024/209.pdf

11. Токарева В.О., Личко В.С. Спадкування об'єктів в мережі Інтернет: досвід західних держав. *Часопис цивілістики*. 2024. № 53. С. 41-46.

Приватний нотаріус Одеського
міського нотаріального округу

Тетяна ДІМІТРОВА

16. квітня
2025р.