УДК 341
DOI: 10.21564/2414-990X.172.353393

Ідентифікація без надмірності у метавсесвіті: баланс між публічним інтересом і вимогами GDPR

Дар'я Анатоліївна Булгакова*
Запорізький інститут економіки та інформаційних технологій,
Кривий Ріг, Україна
**e-mail: dariabulgakova@yahoo.com*

Анотація
Розвиток метавсесвіту формує істотні виклики у сфері захисту персональних даних, кримінального доказування та юридичної відповідальності. З огляду на це набуває актуальності визначення ролі аватарів як цифрових репрезентацій користувачів, здатних розкривати та генерувати біометричні й інферовані персональні дані. Тому метою дослідження є аналіз можливості застосування традиційних підходів до розслідування злочинів у метавсесвітах, а також у визначенні впливу регулювання захисту персональних даних на процес доказування. Для її досягнення застосовано в основному порівняльно-правовий, системно-структурний, формально-юридичний та функціональний методи. Отримані результати демонструють обмеженість традиційних підходів до розслідування злочинів, тому що орієнтовані на дані кінцевих пристроїв. Обґрунтовано необхідність переходу до середовищно-орієнтованих методів доказування. Визначено, що аватари виступають джерелом складних персональних даних, включаючи біометричні. Розкрито обмежувальну роль регулювання захисту даних та проблему формальної згоди користувачів в умовах домінування платформ. На основі практики ЄС, зокрема Республіки Хорватія, доведено потребу в адаптації правових механізмів. Подальші дослідження рекомендовано спрямувати на розробку спеціалізованої тактики доказування у сфері метавсесвіту, удосконалення обробки біометричних даних, формування стандартів з оцінки таких доказів та забезпечення принципів прозорості, мінімізації і пропорційності.

Ключові слова: метавсесвіт; аватар; персональні дані; біометричні дані; інферовані дані; захист персональних даних; Загальний регламент про захист даних.

Identification Without Redundancy in the Metaverse: Balance between Public Interest and GDPR Requirements

Daria A. Bulgakova*
Zaporizhzhia Institute of Economics and Information Technologies,
Kryvyi Rih, Ukraine
**e-mail: dariabulgakova@yahoo.com*

Abstract
The development of the metaverse creates significant challenges in the field of personal data protection, criminal evidence, and legal liability. In this regard, the definition of the role of avatars as digital representations of users, capable of revealing and generating biometric and inferred personal data, becomes relevant. Therefore, the purpose of the study is to analyze the possibility of applying traditional approaches to the investigation of crimes in metaverses, as well as to determine the impact of personal data protection regulation on the evidence process. To achieve this, comparative legal, systemic-structural, formal-legal, and functional methods were used. The results obtained demonstrate the limitations of traditional approaches to investigating crimes because they are focused on end-device data. The need to transition to environment-oriented methods of evidence is substantiated. It is resolved that avatars are a source of complex personal data, including biometric data. The restrictive role of data protection regulation and the problem of formal user consent in conditions of platform dominance are revealed. Based on the practice of the EU, in particular the Republic of Croatia, the need for adaptation of legal mechanisms has been proven. Thus, further research is recommended to be directed towards the development of specialized tactics of evidence in the field of metauniverse, improvement of biometric data processing, formation of standards for the assessment of such evidence, and ensuring the principles of transparency, minimization, and proportionality.

Keywords: metaverse; avatar; personal data; biometric data; inferred data; personal data protection; General Data Protection Regulation.

Вступ

Розвиток метавсесвіту як інтерактивного та цифрового середовища призводить до радикального ускладнення соціальних, технічних і правових взаємодій. Аватари, які використовуються користувачами для участі у віртуальних світах, перестають бути лише візуальними образами і перетворюються на носії персональних, у тому числі біометричних та інферованих даних. Це створює значні ризики незаконного профілювання, дискримінації, порушення приватності та зловживань, особливо за відсутності прозорих механізмів інформування і дійсно вільної згоди.

Кримінальні правопорушення у метавсесвітах відбуваються в умовах технічної опосередкованості дій, розподілених систем зберігання даних і часткової автономії аватарів та алгоритмів. Традиційні підходи до розслідування, що ґрунтуються на аналізі даних кінцевих пристроїв, є фрагментарними та віктимологічно зміщеними. Вимоги GDPR щодо мінімізації, пропорційності та правової підстави опрацювання персональних даних істотно обмежують можливості збору й використання цифрових доказів.

У результаті виникає комплексна проблема: як забезпечити ефективне кримінальне розслідування і відповідальність у метавсесвіті, не порушуючи фундаментальних прав на захист персональних даних, свободу згоди та принцип правової визначеності.

Метою дослідження є комплексний правовий аналіз метавсесвіту як продовження вебу з точки зору захисту персональних даних, кримінального доказування та відповідальності, з особливим акцентом на правовий статус аватарів і межі допустимого опрацювання біометричних та інферованих даних відповідно до вимог GDPR.

Для досягнення цієї мети у роботі поставлено такі завдання:

- проаналізувати еволюцію концепції метавсесвіту та його технічну архітектуру в контексті правового регулювання;
- оцінити придатність традиційних підходів до кримінального розслідування у віртуальних середовищах;
- визначити значення GDPR як матеріального обмеження кримінального доказування;
- дослідити роль аватарів як цифрових репрезентацій особи та їх потенціал для ідентифікації і профілювання користувачів;
- обґрунтувати необхідність переосмислення відповідальності платформ і моделей згоди в умовах домінування цифрових систем на прикладі хорватського кейсу.

Огляд літератури

Актуальна література з проблематики метавсесвіту, аватарів і захисту персональних даних базується насамперед на Регламенті (ЄС) 2016/679, ухваленому European Parliament та Council of the European Union (далі – GDPR) [1], який встановлює фундаментальні принципи законності, пропорційності та мінімізації опрацювання персональних даних і визначає правові межі їх використання у цифрових середовищах. На цьому нормативному значенні сучасні дослідження, зокрема робота Almomani та ін. [2], аналізують етичні виклики, пов'язані з AI-керованими аватарами, звертаючи увагу на ризики непрозорого збирання біометричних і поведінкових даних. Концептуальні

витоки самого явища метавсесвіту простежуються у художньому творі Snow Crash Ніла Стівенсона [3], де аватар постає як цифрове продовження особистості, що згодом було емпірично підтверджено в аналізі соціальних і правових конфліктів у віртуальному світі Second Life у праці The Second Life Herald [4].

Подальший розвиток тематики пов'язаний із безпековим виміром метавсесвіту, що відображено у звіті Interpol [5], де наголошується на складності атрибуції дій та транскордонному характері правопорушень, а також у доповіді Europol [6], яка акцентує на залежності правоохоронних органів до вимог GDPR для доступу до платформних даних. Дослідницькі висновки корелюють із результатами scoping-дослідження Gymez-Quintero та ін. [7], які доводять, що метавсесвіт не створює нових видів злочинів, але трансформує способи їх вчинення.

Додатковий напрям цієї праці присвячений цифровим репрезентаціям особи, зокрема феномену ghostbots, проаналізованому Harbinja, Edwards і McVey [8], а також правовому режиму біометричних даних померлих осіб у контексті GDPR, що досліджували D. Bulgakova і V. Bulgakova [9].

Питання приватності аватарів набуло подальшого розвитку в роботі Sorrentino і Lypez-Guzmбn [10], які наголошують на особливій чутливості інферованих даних у метавсесвіті.

У доктрині права ЄС Bulgakova і Deruma [11] аналізують відповідальність онлайн-посередників, тоді як Majcher [12] підкреслює проблему узгодженості між правом захисту персональних даних і конкурентним правом в умовах платформної домінації.

Теоретичні основи аналізу злочинності у віртуальних світах [13] залишаються актуальними для сучасних метавсесвітів, що підтверджується новітніми дослідженнями кіберзлочинності у цих середовищах [14].

Практичний вимір застосування принципів GDPR ілюструє рішення Agency for Personal Data Protection [15] щодо надмірної обробки персональних даних, а також національне регулювання, ухвалене Republic of Croatia [16], яке демонструє деталізацію вимог захисту даних. Завершальним є аналіз судової практики Суду ЄС, що здійснили D. Bulgakova і V. Bulgakova [17], що підтверджує автономний і пріоритетний характер права на захист персональних даних незалежно від технологічного контексту.

Матеріали та методи

Методологічну основу дослідження становить сукупність загальнонаукових і спеціально-юридичних методів пізнання, застосування яких зумовлене

міждисциплінарним характером проблематики метавсесвіту, що поєднує елементи інформаційного права, кримінального права, права захисту персональних даних та цифрової судової експертизи.

Діалектичний метод використано для аналізу метавсесвіту як динамічного цифрового середовища, що розвивається еволюційно, а також для виявлення взаємозв'язку між технологічним прогресом, трансформацією соціальних практик і змінами у правовому регулюванні.

Формально-юридичний метод застосовано для тлумачення норм GDPR, актів права Європейського Союзу, національного законодавства Республіки Хорватія, а також їх співвідношення в опрацюванні персональних і біометричних даних у метавсесвітах.

Системний метод дав змогу розглянути метавсесвіт як багаторівневу соціально-технічну систему, в якій взаємодіють користувачі, аватари, цифрові платформи, алгоритмічні механізми та правові норми, а також проаналізувати кримінальне доказування як елемент цієї системи.

Порівняльно-правовий метод використано для зіставлення підходів міжнародних організацій, практики застосування GDPR та окремого національного кейсу щодо прозорості та мінімізації даних із метою виокремлення універсальних принципів і нормативних розбіжностей.

Логіко-догматичний метод застосовано для формулювання правових категорій – понять «аватар», «цифровий двійник», «інферовані дані», «свобода згоди», а також для аргументації можливості обмеженої правосуб'єктності аватарів у метавсесвіті.

Метод правового моделювання мав значення при розробленні теоретичних підходів до відповідальності платформ і користувачів у метавсесвіті, а також для прогнозування правових наслідків різних моделей опрацювання даних і архітектури цифрових середовищ.

Кейс-метод застосовано під час аналізу практики застосування принципу мінімізації даних у межах конкретної правової ситуацій, що дозволило екстраполювати висновки на проблематику кримінального доказування у метавсесвітах.

Міждисциплінарний підхід використано шляхом залучення напрацювань у сфері інформаційних технологій, цифрової форензики, штучного інтелекту та соціальних наук, що забезпечило комплексний характер дослідження та релевантне відображення технічної опосередкованості дій у віртуальних середовищах.

Результати та обговорення

Витоки еволюції метавсесвіту

Пропонується уявити, що ви опиняєтеся в масово багатокористувацькій онлайн-грі (MMO), де аватари гравців – не просто графічне представлення, а носій даних, здатних інферувати чутливу інформацію про користувача. Такі цифрові альтер-его відкривають нові горизонти для ігор, створюючи складні юридичні питання, а саме: як платформи забезпечують безпечне опрацювання даних, захист від незаконного профілювання та зловживань через зовнішні характеристики аватарів. Наведені правові занепокоєння є актуальними, адже механізми GDPR [1] можуть виявитися недостатніми, особливо коли доступ до важливих сервісів прив'язаний до надання згоди на опрацювання персональних даних. Тому пропонується дослідити історичні витоки такого феномену, як метавсесвіт, зокрема, у сферах даних та ідентичності.

Відповідно до дослідження, перші концептуальні передумови метавсесвіту простежуються в текстових MUD-системах кінця 1970-х – початку 1980-х рр. Вони заклали основу для цифрової ідентичності та спільної віртуальної взаємодії. У 1990-х рр., із розвитком комп'ютерної графіки, з'явилися такі платформи, як Active Worlds та Ultima Online, що впровадили постійні віртуальні активи та зачатки цифрових економік [2, 130612–130613].

Поняття «метавсесвіт» було введене Нілом Стівенсоном у його науково-фантастичному романі Snow Crash [3], де воно описується як повністю занурюване тривимірне віртуальне середовище, в якому користувачі взаємодіють один з одним та з програмними агентами у вигляді налаштовуваних аватарів. Стівенсон зазначає, що терміни аватар та метавсесвіт є його власними винаходами, створеними для заміни громіздкого виразу «віртуальна реальність». У його метавсесвіті цифровий світ організований навколо центральної вулиці, відомої як Street, на планеті з окружністю 65 536 км (2^{16} км). Віртуальна власність належить вигаданій організації Global Multimedia Protocol Group (MMORPG), а користувачі можуть купувати землю та зводити будівлі. Доступ до метавсесвіту забезпечується через персональні термінали, що проєктують високоякісне VR-зображення на окуляри, або через публічні термінали у спеціальних кабінах, причому досвід подається від першої особи. Користувачі можуть залишатися постійно під'єднаними до метавсесвіту, отримуючи прізвисько через нетиповий зовнішній вигляд. Аватари можуть мати різноманітні форми, обмеження накладається лише на зріст, щоб уникнути надмірного масштабування. Рух у метавсесвіті відтворює реальні способи пересування, як-от пішки або за допомогою монорейкової лінії тощо.

World of Warcraft – одна з найпопулярніших MMO у світі. За чотири місяці після релізу напередодні Дня подяки 2004 р. WoW набрала 1,5 мільйона підписників лише у Північній Америці, а до кінця 2005 р. – 5 мільйонів у всьому світі [4]. Як показує такий приклад MMO, гравці створюють власні сюжети та соціальні взаємодії, які розробники не завжди можуть передбачити. Так, у метавсесвіті учасники можуть об'єднуватися, планувати, співпрацювати або конфліктувати поза межами програмних сценаріїв. До прикладу, для розслідування злочинів це означає, що аналіз лише ігрових об'єктів чи логів недостатній, тому потрібно враховувати соціальні мережі, поведінкові патерни та взаємодію між учасниками віртуального світу. Крім того, як у MMO гравці змінюють сюжет та створюють власні правила, так і зловмисники у метавсесвіті можуть використовувати ігрові механіки та соціальні взаємодії для прихованих дій, таких як шахрайство, торгівля забороненими ресурсами або координація атак у віртуальному світі.

Отже, метавсесвіт надає користувачам нові способи взаємодії через спільний інтерфейс. Як і в історії інтернету та веббраузерів, ключовим фактором широкого впровадження є не сама технологія, а її доступність та простота використання для кінцевих користувачів. Наприклад, швидке поширення інтернету та вебтехнологій у середині 1990-х було зумовлене не самою технологією, а доступністю та простотою використання веббраузерів (зокрема Internet Explorer у Windows 95), що створило критичну масу користувачів. Це стимулювало реєстрацію нових доменів і створення сайтів, посилюючи взаємне зростання попиту та пропозиції онлайн-сервісів. Веб став домінуючою платформою завдяки простоті HTML/HTTP, доступності хостингу та можливості поєднувати роботу і розваги, що відображає еволюційний, а не революційний характер розвитку цифрових технологій. Пізніше аналогічний принцип пояснює розвиток мобільних технологій і смартфонів, де ключове значення має постійна доступність для різних видів використання, а не первісне призначення пристрою.

Таким чином, метавсесвіт базується на багаторівневій архітектурі, що поєднує апаратну інфраструктуру, обчислювальні ресурси та інтелектуальні інтерфейси [2, 130613]:

1. Розширена реальність (XR) об'єднує VR, AR та MR і забезпечує сенсорну імерсію, зокрема через просторовий звук і тактильний зворотний зв'язок.
2. Блокчейн і децентралізація створюють умови для прозорого володіння цифровими активами та автономного управління, водночас ускладнюють питання відповідальності та регулювання.

3. Edge-обчислення та мережі 5G/6G мінімізують затримки, що критично важливо для AI-аватарів у реальному часі.
4. Штучний інтелект і машинне навчання забезпечують процедурну генерацію контенту, інтелектуальних NPC та персоналізовані взаємодії, проте створюють ризики непрозорості, упередженості та зловживань.

Метавсесвіт у системі сучасного (кримінального) права

Інтерпол [5] характеризує метавсесвіт як наступний етап розвитку інтернету. З правового погляду, така характеристика є ключовою, адже визнає метавсесвіт як еволюцію, а не радикальну зміну. Так, Інтерпол непрямо відкидає ідею про те, що діяльність у занурювальних віртуальних середовищах існує поза межами чинного законодавства. Натомість поведінка в метавсесвіті залишається пов'язаною з наявними інфраструктурами як підключення до інтернету, управлінням платформами та взаємодією через апаратні засоби, які вже регулюються на національному та міжнародному рівні.

Із правового погляду, це ставить низку важливих питань щодо атрибуції дій, достовірності доказів, персональної ідентичності та тілесної недоторканності, особливо там, де сенсорне занурення стирає межі між психологічною та фізичною шкодою.

Європол [6] пропонує схоже, але технічно менш детальне визначення, зокрема вводить концепцію цифрового двійника» як візуально схожого представника користувача у симульованому просторі. Це має правове значення, оскільки підкреслює, що аватари та цифрові двійники функціонують як розширення особи, а не як автономні суб'єкти права, у якому користувачі, представлені аватарами, взаємодіють у віртуальних просторах, відокремлених від фізичного світу. Тому завдання перед законодавцями та судами застосувати наявні правові принципи – юрисдикцію, відповідальність, згоду та шкоду – до нових форм взаємодії. Відповідно, дії, здійснені через такі представництва, можуть підпадати під сучасні доктрини кримінальної відповідальності, цивільної відповідальності та захисту прав людини.

Таким чином, метавсесвіт, як і MMO, створює складну мережу соціальних і технічних взаємодій, де злочини можуть залишатися невидимими, якщо розслідування обмежується лише ігровими логами чи окремими об'єктами. Тому для ефективного досягнення завдань відповідальності у правовій площині у метавсесвіті слід застосовувати комбінований підхід, що включає: 1) технічну експертизу пристроїв і серверних логів; 2) аналіз соціальних зв'язків і групової поведінки; 3) вивчення патернів комунікацій і взаємодій; 4) врахування непередбачуваних дій користувачів, які можуть змінювати розвиток подій у світі.

Дослідження Gymez-Quintero та інших [7] дає систематичну оцінку злочинних загроз, пов'язаних із розвитком метавсесвіту, підкреслюючи імплікації для правоохоронних органів та кримінальної політики. Одним із найважливіших висновків є те, що традиційні підходи до розслідування, які базуються винятково на інформації з кінцевих пристроїв учасників (endpoint-only підхід), є недостатніми й не можуть адекватно відображати складність і масштаби злочинності в таких середовищах.

Наприклад, форензика кінцевих пристроїв – end-point forensics – може надати інформацію про злочини (аналогічно до аналізу смартфонів чи ПК), але така інформація обмежена, адже залежить від налаштувань програмного забезпечення, дає лише частковий зріз активності, переважно фокусується на пристроях жертв, що може створювати спотворений образ – victimological bias.

Окрім того, у рамках класичних кримінальних розслідувань в онлайн-середовищах слідчі часто зосереджуються на даних, які можна безпосередньо вилучити з пристроїв жертви, наприклад, логах із мобільного телефону, комп'ютера або VR-шолома. Проте, як показало дослідження Gymez-Quintero зі співавторами [Там само], дані з VR-пристроїв та іншого обладнання, що забезпечує взаємодію в метавсесвіті, мають суттєві обмеження. По-перше, неповнота. Записи периферійних пристроїв – VR-шоломів, контролерів – не охоплюють усі дії учасників і не фіксують контекст взаємодій між аватарами, які можуть бути критичними для розслідування. По-друге, суб'єктивність. Такі дані часто відображають лише сенсорний досвід конкретного користувача, а не об'єктивну послідовність подій або поведінку інших учасників. По-третє, віктимологічне зміщення. Фіксація лише поведінки жертви може створювати спотворену картину подій, що ускладнює визначення наміру, ролі та відповідальності інших сторін.

Розслідування злочинів у метавсесвіті відбувається в умовах підвищеної цифрової складності, де поведінка користувачів опосередковується аватарами, а події фіксуються в розподілених технічних системах. У такому середовищі природною реакцією правоохоронних органів є прагнення до максимальної ідентифікації суб'єктів шляхом збору, агрегації та кореляції великих масивів персональних даних. Проте застосування такого підходу нівелюється жорсткими обмеженнями GDPR, які істотно впливають на допустимі межі кримінального доказування.

Опрацювання персональних даних і доказування: підхід GDPR

Відповідно до ст. 5(1)(c) GDPR, персональні дані мають бути адекватними, релевантними та обмеженими тим, що є необхідним для досягнення визна-

ченої мети опрацювання. У контексті метавсесвіту цей принцип набуває особливого значення, оскільки цифрове середовище технічно дозволяє фіксувати детальні дані про поведінку користувачів, включно з біометричними показниками, рухами тіла, зоровими реакціями та просторовою навігацією.

Дослідження Gymez-Quintero зі співавторами, показує, що орієнтація на дані з кінцевих пристроїв користувачів (VR-гарнітури, haptic suits, AR-додатки) створює ілюзію повноти доказів, тоді як на практиці такі дані є фрагментарними, суб'єктивно забарвленими та віктимологічно зміщеними. З точки зору GDPR, масовий збір подібних даних без чіткої прив'язки до конкретної кримінальної гіпотези може розглядатися як непропорційний та надмірний, що ставить під сумнів їх допустимість як доказів.

Стаття 6 GDPR вимагає наявності чіткої правової підстави для опрацювання персональних даних. Навіть у межах кримінального провадження сама по собі потенційна корисність даних для розслідування не є достатнім виправданням їх збору. Тому в метавсесвіті межа між персональними даними, технічними логами та поведінковими патернами є викривленою.

Як підкреслюють Gymez-Quintero та ін., значна частина злочинів у метавсесвіті (зокрема сексуальні, фінансові та шахрайські) може бути розслідувана ефективніше через аналіз системних даних середовища як серверних логів, транзакційних записів, міжплатформних взаємодій без необхідності прямої ідентифікації користувачів на ранніх етапах розслідування [7]. На думку автора цієї роботи, такий підхід краще узгоджується з вимогами GDPR, адже дозволяє відокремити встановлення факту правопорушення від виокремлення особи правопорушника.

У зв'язку з цим розслідування у метавсесвіті повинно виходити за межі кінцевих пристроїв і включати більш комплексні джерела доказів, наприклад, серверні логи. Враховуючи те, що метавсвіт функціонує як сервер-клієнтна система, де значна частина подій фіксується централізовано на серверах, то аналіз логів дає змогу відновити хронологію взаємодій між аватарами, ідентифікувати підозрілу поведінку, а також підтвердити зв'язки між окремими подіями, що неможливо зробити лише на основі даних пристрою жертви.

Іншим прикладом є міжплатформна кореляція. Оскільки користувачі часто діють одночасно в кількох віртуальних середовищах або сервісах (ігри, соціальні платформи, торгівельні майданчики), ефективне розслідування мусить передбачати кореляцію подій між різними системами, тому що дозволяє встановити, чи та сама особа вчинила аналогічні правопорушення в різних контекстах.

Третім прикладом є фінансові та блокчейн-дані. Як правило, злочини у метавсесвіті пов'язані з обігом віртуальних активів, які мають реальну вартість. Так, фінансові транзакції, записи блокчейн-мереж та RMT-операції є критично важливими доказами для встановлення зв'язку між віртуальними подіями та реальними економічними наслідками.

Наступне – це аналіз поведінки аватарів. Нестандартні моделі взаємодії, повторювана поведінка або систематичні шаблони можуть вказувати на злочинні схеми. Дослідження таких моделей дозволяє не лише виявити правопорушення, а й документувати намір та методологію дій злочинця.

Більше того, дослідження Harbinja, Edwards та McVey [8] пропонує до розгляду феномен ghostbots, трактуючи його не просто як технологічний, а як форма цифрової присутності особи після смерті, яка може існувати й функціонувати саме у віртуальних середовищах і метавсесвітах та виступати суб'єктом взаємодії в метаверсі. Автори показують, що чинне право не визнає ghostbot суб'єктом відповідальності, тому залишається відкритим питання, хто відповідає за дії ghostbot у віртуальному просторі. У світі метаверсу це створює вакуум відповідальності, коли шкода завдається у віртуальному середовищі; дії вчиняє автономна або напівавтономна AI-система; немає чітко визначеного відповідального суб'єкта (розробник, спадкоємець, платформа). Тому сучасне право не має ефективної моделі відповідальності за дії цифрових аватарів і AI-репрезентацій особи, зокрема ghostbots, що створює ризик безкарності та зловживань у метавсесвітах. Наведене концептуально пов'язується з підходом, який запропонували D. Bulgakova та V. Bulgakova [9].

Так, обидва напрями досліджень виходять за межі суто технологічного розуміння цифрових об'єктів. Якщо Harbinja, Edwards та McVey [8] розглядають ghostbots як форму цифрової присутності особи після смерті, яка може активно функціонувати у віртуальних середовищах і метавсесвітах, то D. Bulgakova та V. Bulgakova [9] аналізують біометричні дані померлих як об'єкт особистих немайнових прав і доводять, що навіть після смерті такі дані залишаються юридично значущими та потребують захисту. Також висновки досліджень збігаються у визнанні того, що цифрові репрезентації померлої особи (біометричні дані, аватари, ghostbots) не є нейтральними даними. Вони тісно пов'язані з особистістю людини, її ідентичністю та гідністю. У метаверсі це набуває особливої уваги, адже ghostbots можуть виступати суб'єктами взаємодії, а саме: спілкуватися з іншими користувачами, впливати на їх поведінку, брати участь у віртуальних подіях або навіть у економічних процесах. Окрім того, автори досліджень виявляють

нормативний розрив у праві. Harbinja, Edwards та McVey [8] підкреслюють, що чинне право не дає чіткої відповіді, хто має відповідати за його дії у метаверсі; здобутки D. Bulgakova та V. Bulgakova [9] підтверджують, що правовий режим біометричних даних померлих осіб залишається фрагментарним і непристосованим до нових цифрових практик, особливо коли такі дані використовуються для створення або підтримки цифрових двійників. Отже, праці науковців підкреслюють необхідність переосмислення підходів до персональних даних, відповідальності та правосуб'єктності у цифрових і віртуальних середовищах.

Стаття 25 GDPR закріплює принцип захисту даних за замовчуванням і за задумом (privacy by design and by default), який має прямі наслідки для архітектури метавсесвітів і, відповідно, для можливостей кримінального доказування. Якщо платформи проєктуються таким чином, що від самого початку обмежують збереження персональних даних і надають пріоритет агрегованим або псевдонімізованим формам логування, то матиме місце звуження простору для традиційних персоналізованих доказів. Але, Gymez-Quintero та ін. [7] показують, що таке обмеження необов'язково знижує ефективність розслідувань. Навпаки, воно стимулює перехід від індивідуально-орієнтованого доказування до середовищно-орієнтованого аналізу, де ключовими є повторювані патерни поведінки аватарів, аномалії у цифрових транзакціях, структурні вразливості платформ, взаємозв'язки між подіями у різних частинах метавсесвіту. Отже, метавсесвіт не створює принципово нових злочинів, а посилює наслідки вже відомих форм протиправної поведінки.

Слід зазначити, що GDPR, з іншого боку, є нормативним бар'єром проти перетворення метавсесвіту на середовище постійного спостереження. Закон змушує практиків кримінального права шукати баланс між захистом суспільних інтересів і фундаментальними правами суб'єктів даних, навіть у ситуаціях високого ризику та суспільного резонансу. Саме тому GDPR у контексті метавсесвіту слід розглядати не лише як інструмент захисту приватності, а й як структурне обмеження кримінального доказування, яке змінює саму логіку розслідувань. Він обмежує доказування через надмір, водночас сприяючи розвитку більш витончених, системних та пропорційних методів виявлення і доведення злочинів. У такому змісті GDPR задає доказуванню рамки легітимного та правозахисного розвитку.

Від аватару до суб'єкта

Формально аватар може не мати нічого спільного з реальною зовнішністю користувача. Проте емпіричні дослідження показують, що більшість користувачів створюють аватари, які значною мірою нагадують їх реальний

вигляд. Інші ж наукові дослідження підтверджують, що в багатьох випадках існує такий тісний зв'язок між аватаром і його людським прототипом, що результати розпізнавання аватарів можуть бути використані для ідентифікації реальних осіб, і навпаки [10]. Це відкриває нову сферу так званої віртуальної біометрії, яка доповнює або розширює традиційні біометричні методи за рахунок даних, отриманих у віртуальних середовищах. Наприклад, аватар може розкривати геометрію обличчя, расове або етнічне походження, гендерну ідентичність (залежно від контексту), стан здоров'я, якщо певні захворювання мають зовнішні прояви.

У таких умовах виникає потреба в системах безпеки, здатних функціонувати в контексті інтерреальності та доповненої реальності, що ще більше посилює значення опрацювання та захисту біометричних даних.

Таким чином, ключова проблема полягає в тому, що аватари можуть бути як суттєво відмінними від реальної особи, так і майже повністю її відтворювати. Із розвитком технологій не можна виключати ситуацію, коли зображення аватара стане достатнім для точної ідентифікації конкретної людини, особливо в ситуації обмеженого кола осіб. Така ідентифікація може здійснюватися як самою платформою, так і третіми сторонами. Але політики конфіденційності зазвичай не містять чітких положень щодо таких практик, що породжує серйозні проблеми прозорості. Користувачі не можуть (хоча повинні) передбачити правові наслідки створення та використання аватарів, наприклад, виведення з них чутливих персональних даних, таких як расове походження, стан здоров'я або інші фізичні характеристики.

Аналіз політик конфіденційності провідних платформ метаверсу (зокрема Decentraland, Roblox, Epic Games/Fortnite та Ready Player Me) свідчить про відсутність як згадок про біометричні дані, так і будь-яких процедур отримання згоди на їх опрацювання [10]. Як правило, зображення аватарів не використовуються для конкретних цілей, що формально може пояснювати відсутність вимоги згоди.

Утім ланка проблеми полягає не в задекларованих цілях, а в потенційній правовій кваліфікації даних аватарів. Якщо такі дані почнуть фактично опрацьовуватися, постає принципова проблема: чи слід розглядати їх як звичайні персональні дані, чи як спеціальні категорії персональних даних у розумінні статті 9 GDPR. Від відповіді на це запитання залежатиме як допустимість їх опрацювання, так і межі відповідальності платформ метаверсу та інших учасників цифрової екосистеми.

Навіть якщо опрацювання даних аватарів у метаверсі не підпадає під ст. 9(2)(a) GDPR (явна згода), теоретично вона може бути обґрунтована через

ст. 9(2)(e) у випадках, коли персональні дані були явно оприлюднені самим суб'єктом даних. З іншого боку, така правова кваліфікація залишається вразливою для критики, оскільки оприлюднення через аватар навряд чи можна вважати достатньо поінформованим. Особливо критичним є те, що платформи майже повністю ігнорують інферовані дані, хоча саме вони створюють найбільші правові та етичні ризики.

Слід зазначити, що біометричні дані можуть формально не оброблятися з метою прямої ідентифікації особи, та платформи не враховують той факт, що поведінкові, візуальні та стилістичні характеристики аватара дозволяють здійснювати вторинну ідентифікацію, профілювання. У такій ситуації навіть за відсутності обов'язку отримувати явну згоду відповідно до ст. 9 GDPR, принцип прозорості вимагає належного інформування користувачів про наслідки налаштування та використання аватара.

Доречним є приклад міжплатформної інтероперабельності аватарів, коли сервіси дозволяють створювати гіперреалістичні аватари на основі фотографій користувачів за допомогою автоматизованого опрацювання. Цей процес об'єктивно може включати біометричні елементи, зокрема геометрію обличчя. Водночас політики конфіденційності таких сервісів не містять чітких згадок про опрацювання біометричних даних, не пояснюють можливості інферування та допускають передачу цих даних третім сторонам без явної згоди суб'єкта. Бізнес-модель подібних сервісів базується саме на поширенні аватарів між платформами, що суттєво підвищує ризики порушень прав користувачів.

Додаткову складність створює роль учасників опрацювання даних. Платформа, що отримує аватар, може спочатку виступати як процесор, але згодом, наприклад, шляхом інферування особи користувача на основі біометричних характеристик аватара, фактично ставати контролером. Це особливо небезпечно у випадках, коли йдеться про неповнолітніх або представників соціальних і етнічних меншин, які можуть зазнавати дискримінації, переслідувань або інших форм віртуальної злочинності на основі зовнішніх характеристик аватара. Право бути поінформованим у такому контексті є ключовим інструментом активного наділення користувачів контролем над власними даними.

Отже, аватари дедалі більше перетворюються на носіїв біометричних даних, тоді як користувачі залишаються необізнаними щодо реального обсягу інформації, яку можна з них вивести. Виникає потреба не лише у тлумаченні норм GDPR, а й їх координації з новими регуляторними актами у сфері штучного інтелекту та цифрових середовищ, а також посиленні відповідальності платформ за запобігання шкоді та злочинності у метаверсі.

Водночас, коли згода є умовою надання послуги, критеріями оцінки є домінування платформи та суттєвий характер послуги, щоб уникнути ситуації, коли користувач, відмовившись надати згоду на несправедливу угоду, втрачає доступ до необхідного сервісу без будь-якої альтернативи. У розумінні метавсесвіту така практика набуває особливої актуальності, адже цифровий аватар стає засобом взаємодії з платформою, а відмова надати згоду на обробку персональних та інферованих даних може означати неможливість користуватися соціальною мережею чи віртуальним середовищем, що фактично монополізується домінуючим провайдером. Наприклад, у справі *Google Shopping* 2017 р. Єврокомісія встановила, що Google зловжила домінуючим становищем на ринку пошукових систем, надаючи пріоритет власному сервісу порівняння цін і обмежуючи доступ конкурентів [11].

Умови свободи згоди вимагають, щоб користувачі мали реальну можливість обрати іншу опцію. Проте у ринку, де домінує потужна платформа, альтернативи часто відсутні, що створює асиметрію залежності користувача від платформи: проблема не у відносинах сили, а у високому рівні залежності від конкретного сервісу [12, 238-241].

Статті 13 та 14 GDPR покладають на контролерів обов'язок надавати чітку та вичерпну інформацію про опрацювання персональних даних, незалежно від джерела їх отримання. Користувачі мають бути поінформовані про ризики інферування біометричних даних через аватари, і така інформація має надаватися не лише при створенні аватара, а й під час кожного його використання на новій платформі. Інакше політики конфіденційності провайдерів метавсесвіту дозволяють обходити суворі вимоги щодо спеціальних категорій персональних даних, створюючи можливості для правопорушень у віртуальному середовищі.

Метавсесвіт агрегує та уніфікує сервіси, створюючи відчуття інтерактивного та зануреного досвіду, але не створює принципово нових типів сервісів чи кримінальних можливостей, адже змінює спосіб їх подання і взаємодії. Таким чином, метавсесвіт змінює способи вчинення та реалізації наявних злочинів у цифровому середовищі, утім, не створює принципово нових видів кримінальної діяльності.

Феномен метавсесвіту вказує на необхідність адаптації наявних норм, особливо у сфері кримінального права, цифрової судової експертизи, захисту персональних даних та прав людини. Метавсесвіт, таким чином, постає питанням регуляторної безперервності, а не абсолютно новою юридичною сферою.

Автор цієї роботи розглядає метавсесвіт як розширення вебу, що включає більше протоколів прикладного рівня, доступних через різні клієнтські

інтерфейси та пристрої. Ці пристрої (VR/AR) агрегують сервіси під єдиним інтерфейсом, подібно до того, як браузери у 1990-х дозволили користувачам працювати з різними вебсайтами через один клієнт, де цифровий двійник – це необов'язково багатофункціональна віртуальна копія об'єкта чи особи, а елемент, який дозволяє ідентифікувати оригінал у метавсесвіті. Ідентифікація може здійснюватися через токени або поведінкові моделі, які імітують властивості оригіналу.

Але що відбувається технічно, якщо користувач вирішує озброїти свого аватара віртуальним мечем і витратити на нього гроші? Користувачі віртуальних світів сприймають об'єкти як зображення на своїх екранах, що складаються з пікселів, згенерованих даними. Зовнішній вигляд та властивості віртуального об'єкта визначаються записом у одній базі даних (item-database), тоді як запис в іншій базі даних (character-database) встановлює, які віртуальні об'єкти належать конкретному користувачу. Ці дані зберігає провайдер послуг на центральних серверах [13, 97].

На думку Pandey [14, 136], аватари у метавсесвіті фактично є цифровим втіленням користувача, але не мають власної юридичної особистості. Це створює складнощі у встановленні кримінальної відповідальності, коли аватар здійснює протиправні дії: чи притягати до відповідальності користувача, який його контролює, чи вважати аватар частиною системи, що має автономні реакції. Автор підкреслює, що надмірне автоматичне покладання відповідальності на користувача може стримувати розвиток метавсесвіту, тоді як ігнорування дій аватара створює безкарність. Відповідно, пропонується застосування гібридного підходу: аватар може мати обмежені «правові санкції» (тимчасове блокування або видалення), а відповідальність користувача встановлюється залежно від рівня контролю та передбачуваності дій аватара.

Тому критичною для правового дискурсу є концепція надання аватару в метавсесвіті певної правосуб'єктності (legal personality), який може нести обмежену юридичну відповідальність, означаючи, що аватар сам по собі міг би підлягати санкціям, наприклад, втрата правового статусу аватара у вигляді тимчасової або постійної втрати можливості брати участь у певних функціях метавсесвіту; віртуальний арешт, який може полягати в обмеженні дій аватара на певний час у віртуальній в'язниці; видалення аватара, а саме знищення цифрового облікового запису, який представляє аватара; блокування користувача у вигляді заборони реальній особі створювати нові аватари або користуватися метавсесвітом певний час.

Слід також підкреслити складність атрибуції провини. Так, дії аватара не завжди можна віднести до реальної особи, яка його контролює. Наприклад,

якщо аватар підхопив шкідливе програмне забезпечення (вірус) і внаслідок цього скоїв протиправні дії, виникає запитання: хто відповідає – користувач чи спрацював автономний механізм? Тому метавсесвіт потребує правових механізмів та захисту, які дозволяють диференційовано оцінювати різні ситуації, розмежовуючи відповідальність користувача і автономні дії аватара.

Така диференціація відповідальності неможлива без визнання технічної опосередкованості дії у віртуальних середовищах. На відміну від офлайн-світу, де між наміром і дією зазвичай існує прямий зв'язок, у метавсесвітах цей зв'язок розривається програмним кодом, алгоритмами, мережевими затримками та автоматизованими процесами. Аватар діє як гібридний агент, у якому поєднуються людська воля та машинна автономія.

У запропонованому значенні механічне перенесення класичних правових моделей відповідальності є проблематичним. Принцип вини, що лежить в основі сучасного права, передбачає контроль суб'єкта над своїми діями. У випадках, коли поведінка аватара визначається збоями системи, втручанням стороннього коду або дизайнерськими рішеннями платформи, такий контроль є частковим або взагалі відсутнім. Відповідно, покладання повної відповідальності на користувача виглядає непропорційним і несправедливим.

Тому є необхідність процедурного підходу до врегулювання конфліктів у метавсесвітах. Мова не лише про фіксацію порушення, а про встановлення контексту: технічних логів, архітектури взаємодії, ролі автоматизованих систем і можливих дефектів платформи. Без таких процедур будь-яке покарання ризикує перетворитися на довільний акт влади з боку оператора середовища.

Більше того, проблема атрибуції вини безпосередньо пов'язана зі статусом самої платформи. Якщо метавсесвіт визнається лише приватною грою, відповідальність може перекладатися виключно на користувача. Якщо ж він розглядається як соціально значущий простір, у якому відбуваються економічні, культурні та комунікативні процеси, то й платформа повинна нести частину відповідальності – як архітектор умов дії та як гарант мінімальних процедур справедливості.

На додаток, у віртуальному світі межа між рольовою грою та реальним завданням шкоди є розмитою, а апеляція до рольплею часто використовується для виправдання зловживань і насильства. На думку автора цієї роботи, поведінка, яку гравець трактує як постановну, іншими ж, особливо підлітками, може сприйматися як приниження та психологічна агресія. Те саме стосується серйозніших форм грифінгу, наприклад, вимагання, погроз, економічного тиску, які маскуються під частину гри, але мають реальні

емоційні й матеріальні наслідки. Отже, не вся поведінка, яка прикривається рольплеєм, є етично або соціально прийнятною, особливо в середовищі, де присутні неповнолітні, а віртуальні дії можуть спричиняти справжню травму. Це твердження ставить під сумнів висловлювання «це лише гра» і підкреслює потребу у відповідальності, межах та регуляції поведінки у віртуальних спільнотах.

Наприклад, грифінг як феномен деструктивної поведінки може набувати системної, майже інфраструктурної форми, а не бути лише «поганою поведінкою окремих гравців». Більше того, можуть бути прояви і пасивного грифінгу – створення середовища, яке саме по собі стає ворожим, травматичним або економічно токсичним. Грифінг у віртуальних світах впливає на реальні доходи, може руйнувати бізнес, створює ризики не лише для вразливих гравців, а й для економічних еліт платформи. Таким чином, «це лише гра» втрачає переконливість. Якщо віртуальна нерухомість має ринкову вартість, а дії сусідів можуть її знецінити через навмисну провокацію, то ми маємо справу не з грою, а з соціально-економічною екосистемою. Таким чином, шкода у віртуальних світах може бути опосередкованою, колективною й «легальною», але від цього не менш реальною. Так, коли онлайн-світ стає значущим для життя людей, його неможливо регулювати виключно логікою гри або приватної власності.

Отже, поєднання метавсесвіту з вимогами GDPR дає можливість ефективніше оцінювати, чи є згода користувача віртуального аватара дійсно вільною, і встановлювати юридичну відповідальність платформ за порушення прав користувачів за умов монополізованих цифрових ринків.

З урахуванням зазначеного пропонується:

1) визначити відповідальність платформ за зовнішні характеристики аватарів, які розкривають біометричну інформацію про користувачів;
2) посилити вимоги до надання інформації про інферовані дані;
3) впровадити механізми контролю, які гарантують можливість відмови від згоди без втрати доступу до альтернативних сервісів;
4) координувати правила GDPR із регуляторними актами у сфері штучного інтелекту та цифрових середовищ, щоб домінування платформи не обмежувало свободу вибору користувача.

Надмірне опрацювання персональних даних: аналіз хорватської справи про призову гру

У Республіці Хорватія мала місце призова гра, яка тривала з 20 листопада по 31 грудня 2020 р. За цей час зареєструвалися 10 548 учасників, з яких

108 осіб мали однакові ім'я та прізвище; серед 5 905 осіб, які відповідали всім умовам участі, 37 мали ідентичні імена та прізвища, а 4 учасники, окрім однакових імен, також проживали в тому самому місті (у двох випадках) [15].

Відповідно до Регламенту про організацію призових ігор [16] організатор призового розіграшу зобов'язаний забезпечити публічність розіграшу та публічне оголошення переможців. Банк як організатор виконав цей обов'язок, передбачивши, що імена переможців будуть оприлюднені на його офіційному вебсайті протягом семи днів з дати проведення розіграшу.

У межах призової гри поняття «ім'я переможця» тлумачилося організатором розширено – як сукупність даних, необхідних для однозначної ідентифікації особи, оскільки саме ім'я та прізвище не завжди дозволяють ідентифікувати конкретну людину. Відповідно, перелік даних для оприлюднення був закріплений у Правилах призової гри та відображений в офіційному протоколі розіграшу.

Крім того, у заявці на участь у призовій грі прямо зазначалося, що персональні дані надаються з метою участі у розіграші. Таким чином, участь у призовій грі, за логікою організатора, передбачала прийняття умов щодо публічного розкриття даних переможців банком як організатором, оскільки таке розкриття було прямо передбачене Правилами призової гри.

Організатор також стверджував, що без публічного оголошення переможців він не міг би виконати свій законний обов'язок щодо прозорості, передбачений Регламентом про організацію призових ігор. Така публічність має на меті підтвердити законність, добросовісність і належне проведення призового розіграшу, а також забезпечити можливість будь-якому учаснику звернутися за судовим захистом у разі сумнівів щодо коректності процедури. Так, компанія пояснила, що з огляду на значну кількість клієнтів, які проживають у великих містах, де поширені однакові імена та прізвища, а інколи й однакові адреси, потрібно було збирати, обробляти та публічно відображати певні персональні дані (зокрема ім'я, прізвище, ОІВ та адресу проживання) для забезпечення однозначної ідентифікації учасників і переможців [15].

Водночас із позиції дослідження та практики застосування GDPR, прозорість призової гри не потребує розкриття особливо чутливих або високоризикових ідентифікаторів, таких як персональний ідентифікаційний номер (далі – ОІВ) або повна адреса проживання. Публічний інтерес у прозорості може бути досягнутий менш інвазивними засобами, наприклад, шляхом використання часткових ідентифікаторів або псевдонімізації.

Хоча банк посилався на національні правила щодо призових ігор, обсяг оприлюднених персональних даних перевищував межі необхідного і пропорційного, що призвело до порушення GDPR. Загальний регламент про захист даних вимагає, щоб національні зобов'язання щодо прозорості тлумачилися і застосовувалися відповідно до права ЄС у сфері захисту персональних даних, а не як виняток із нього.

Важливим є те, що Регламент про організацію призових ігор [15] дійсно встановлює юридичний обов'язок публічного оголошення переможців. Зокрема, ст. 12(2) вимагає публічного характеру розіграшу, а ст. 14(2) прямо зобов'язує організатора оприлюднити ім'я та прізвище переможця і місце проживання.

Отже, публікація певного мінімального обсягу персональних даних має законну підставу, незалежно від згоди суб'єкта даних. Але ця правова підстава не є безмежною.

Відповідно до ст. 4(1) GDPR, персональними даними є будь-яка інформація, що стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи. Стаття 4(2) GDPR визначає опрацювання персональних даних надзвичайно широко, включаючи збір, зберігання та публічне розкриття. У хорватській справі публікація імен, OIB та адрес проживання на сайті банку, беззаперечно, становила опрацювання персональних даних у значенні GDPR.

Ключовим стало не питання законності публікації як такої, а питання обсягу оприлюднених даних. Регламент про організацію призових ігор не вимагає публікації OIB або повної адреси проживання. Будь-яке розкриття даних понад ім'я, прізвище та місце проживання повинно мати окреме обґрунтування та відповідати принципу мінімізації даних за ст. 5(1)(c) GDPR.

Зокрема, орган із захисту даних встановив порушення, а саме: публікація OIB і повної адреси проживання не була необхідною для досягнення мети прозорості й публічної перевірки результатів розіграшу [15]. Аргумент банку про однакові імена та прізвища серед учасників був визнаний непропорційним, оскільки проблему ідентифікації можна було вирішити внутрішніми механізмами без публічного розкриття надмірних персональних даних, які створюють підвищені ризики зловживань, зокрема крадіжки ідентичності.

Національна норма Республіки Хорватія прямо передбачає обов'язок дотримання законодавства про захист персональних даних, що не скасовує вимоги GDPR, а має тлумачитися з ними в гармонії.

Сформульовані у справі напрацювання мають значення, що виходить далеко за межі регулювання призових ігор, оскільки вони чітко ілюструють структурне напруження між вимогами прозорості, публічного інтересу та обмеженнями, встановленими GDPR, яке безпосередньо виявляється й у контексті кримінального розслідування злочинів у метавсесвіті.

Кейс демонструє, що навіть за наявності прямого національного правового обов'язку щодо публічності, опрацювання персональних даних не стає автоматично правомірним у повному обсязі. Визначальним є не сам факт законної мети (прозорість, контроль законності, правовий захист), а пропорційність та мінімізація опрацювання даних. Цей підхід має принципове значення для кримінального доказування у цифрових і віртуальних середовищах.

У метавсесвіті потенційні докази як логи серверів, поведінкові патерни аватарів, біометричні та сенсорні дані, транзакційна інформація, як правило, завжди містять надмірні обсяги персональних даних, значна частина яких не є необхідною для досягнення конкретної доказової мети. Аналогічно до розглянутого кейсу, сам факт легітимної цілі (розслідування злочину, забезпечення публічного інтересу, захист потерпілих) не виправдовує необмеженого збору, збереження або розкриття даних.

Особливо важливим є розуміння про те, що альтернативні, менш інвазивні механізми ідентифікації повинні мати пріоритет над публічним або широким розкриттям даних. У кримінальному процесі це означає, що слідчі органи не можуть обґрунтовувати збір або використання повного масиву метавсесвітніх даних лише складністю ідентифікації суб'єктів у віртуальному середовищі. Як і у справі з призовою грою, проблеми ідентифікації мають вирішуватися внутрішніми, контрольованими та процесуально обмеженими інструментами, а не шляхом розширення обсягу опрацьованих персональних даних. Так, кейс підтверджує ключову тезу дослідження, що GDPR функціонує не як формальне процедурне обмеження, а як матеріальна межа кримінального доказування, яка зберігає свою дію навіть за наявності вагомого публічного інтересу. У метавсесвіті, де межа між приватною поведінкою, публічною взаємодією та технічними метаданими є невизначеною, принцип мінімізації даних стає одним із центральних критеріїв допустимості цифрових доказів.

Отже, практика застосування GDPR у традиційних сферах, зокрема у справі про публікацію даних переможців призової гри, створює нормативну матрицю, яка безпосередньо переноситься на розслідування злочинів у метавсесвіті. Вона підтверджує, що майбутнє ефективного кримінального переслідування у віртуальних середовищах залежить не від максимізації збору даних, а від точного, пропорційного та цільового доказування,

узгодженого з фундаментальними правами на захист персональних даних. Так, GDPR не просто регламентує захист приватності користувачів, а фактично визначає червону лінію, за якою починаються незаконні методи збору цифрових доказів.

Тому, якщо платформи метавсесвіту зберігають усі дані «про всяк випадок» для безпеки або співпраці з правоохоронними органами, це відтворює саме ту модель, яку Суд ЄС визнав несумісною з правом на захист персональних даних у праві ЄС, закріпленим у ст. 8 Хартії ЄС про основоположні права, насамперед у справах про data retention (щодо зберігання трафікових і метаданих, автоматизованої обробки, транскордонної передачі даних) [17].

Висновки

Метавсесвіт не створює принципово нових видів злочинів, але трансформує способи їх вчинення та реалізації, ускладнюючи атрибуцію дій, збирання доказів і визначення відповідальності. Аватари в таких середовищах дедалі більше набувають ознак носіїв персональних і біометричних даних, що підвищує ризики незаконного інферування, дискримінації та порушення приватності користувачів.

Застосування виключно end-point підходів до кримінального розслідування є недостатнім і не відображає реальної складності подій у метавсесвіті. Більш ефективними є середовищно-орієнтовані методи, засновані на аналізі серверних логів, транзакційних даних, поведінкових патернів і міжплатформних взаємодій. Такий підхід краще узгоджується з принципами мінімізації та пропорційності, закріпленими у GDPR.

GDPR у контексті метавсесвіту виступає не лише інструментом захисту приватності, а й матеріальною межею кримінального доказування, яка унеможливлює масовий і невибірковий збір персональних даних навіть за наявності вагомого публічного інтересу. Водночас він стимулює розвиток більш точних, системних і правозахисних методів розслідування.

Домінування окремих платформ ставить під сумнів реальну свободу згоди користувачів на опрацювання персональних і інферованих даних, що потребує посилення вимог до прозорості, інформування та наявності альтернатив. Так, відповідальність платформ за дизайн середовища, характеристики аватарів і механізми опрацювання даних має бути чітко визначена.

Метавсесвіт слід розглядати як простір регуляторної безперервності, у якому наявні правові принципи потребують адаптації. Ефективне правове регулювання метавсесвіту можливе лише за умови балансу між інноваціями, кримінально-правовими інтересами та фундаментальними правами людини.

Хорватський кейс щодо публікації персональних даних переможців призової гри демонструє структурну проблему – використання надмірних унікальних ідентифікаторів під прикриттям легітимної мети. Банк – організатор призової гри посилався на прямий юридичний обов'язок публічного оголошення переможців, передбачений національним законодавством. Для досягнення цієї мети він обрав максималістський підхід до ідентифікації, оприлюднивши не лише ім'я та прізвище, а й OIB та повну адресу проживання. Тобто ключовим стало не питання наявності законної мети, а обсяг і інтенсивність застосованих ідентифікаторів.

Згідно з матеріалами справи, суб'єкт опрацювання виходив із такої презумпції: складність ідентифікації виправдовує розширення масиву персональних даних. У хорватському кейсі це простежується в наявності учасників з однаковими іменами та прізвищами. Проте орган із захисту даних дійшов висновку: проблеми ідентифікації мають вирішуватися внутрішніми, контрольованими та менш інвазивними механізмами, а не шляхом загального або публічного застосування високоризикових ідентифікаторів. Надмірність полягала в публічному розкритті OIB та адреси. GDPR виступає не формальною перешкодою для досягнення легітимної мети, а матеріальним обмеженням допустимих способів її досягнення.

Ця аналогія є особливо релевантною для подальшого аналізу доказування у метавсесвіті, де ані публічний інтерес, ані технічна складність ідентифікації не легітимізують надмірне використання ідентифікаторів. Визначальними критеріями залишаються пропорційність, мінімізація та вибір альтернативних, менш інвазивних засобів ідентифікації – принцип, який має безпосереднє значення і для цифрових, і для віртуальних середовищ.

References

[1] European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union, L 119*, 1-88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[2] Almomani, A., Al-Qerem, A., Alauthman, M., Aldweesh, A., Aoudi, S., & Salloum, S.A. (2025). Ethical Foundations of AI-Driven Avatars in the Metaverse for Innovation and User Privacy. *IEEE Access*, *13*, 130610-130628. https://doi.org/10.1109/ACCESS.2025.3589714.

[3] Stephenson, N. (2011). Snow Crash, Penguin Books Ltd., Bangalore.

[4] Ludlow, P., & Wallace, M. (2007). *The Second Life Herald: the virtual tabloid that witnessed the dawn of the metaverse* (1st ed.). The MIT Press.

[5] Interpol. (2023). Technology assessment report on metaverse. Interpol. Retrieved from https://www.interpol.int/en/News-and-Events/News/2022/INTERPOLlaunches-first-global-police-Metaverse.

[6] Europol. (2023). Policing the metaverse: What law enforcement needs to know, an observatory report from the Europol Innovation Lab. *Publications Office of the*

European Union. Retrieved from https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-lawenforcement-needs-to-know.

[7] Gymez-Quintero, J., Johnson, S. D., Borrion, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futures: The Journal of Policy, Planning and Futures Studies*, *157*, 103338. https://doi.org/10.1016/j.futures.2024.103338.

[8] Harbinja, E., Edwards, L., & McVey, M. (2023). Governing ghostbots. *Computer Law & Security Review*, *48*, 105791. https://doi.org/10.1016/j.clsr.2023.105791.

[9] Bulgakova, D., & Bulgakova, V. (2023). The recognition of the deceased biometric data under personal non-property rights in terms of the General Data Protection Regulation. *Bulletin of the Penitentiary Association of Ukraine, 1*, 22-34. https://doi.org/10.34015/2523-4552.2023.1.03.

[10] Sorrentino, G., & Lypez-Guzmán, J. (2025). Rethinking privacy for avatars: biometric and inferred data in the metaverse. *Frontiers in Virtual Reality*, *6*. https://doi.org/10.3389/frvir.2025.1520655.

[11] Bulgakova, D., & Deruma, S. (2023). The liability of online intermediaries under European Union law. *Kyiv-Mohyla Law and Politics Journal*, *8-9*, 1-43. https://doi.org/10.18523/kmlpj303154.2023-8-9.1-43.

[12] Majcher, Klaudia. (November 23, 2023) ‹A Data Protection Law Perspective on Sectional Coherence›, *Coherence between Data Protection and Competition Law in Digital Markets*, Oxford Data Protection & Privacy Law. Oxford Academic. https://doi-org.ezproxy.its.uu.se/10.1093/oso/9780198885610.003.0007.

[13] Cornelius, K., & Hermann, D. (2011). *Virtual Worlds and Criminality* (1st ed.). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-20823-2.

[14] Pandey, P. (2025). Bits and Bytes Betrayal: Unravelling the Dark Threads of Cybercrime in the Metaverse. In N. Pitropakis & S. Katsikas (Eds.). *Security and Privacy in Smart Environments*, *14800*, 120-148. https://doi.org/10.1007/978-3-031-66708-4_6.

[15] Agency for Personal Data Protection. (December 31, 2021). Decision on excessive processing of personal data of prize draw winners (National case reference: Decision 29-06-2022 (bank)). Zagreb, Croatia. Retrieved from https://azop.hr/wp-content/uploads/2022/09/Prekomjerna-obrada-osobnih-podataka-od-strane-banke.pdf.

[16] Republic of Croatia. (2025). Regulation on organizing prize games (Pravilnik o priređivanju nagradnih igara). Narodne novine, No. 125/2025. Retrieved from https://narodne-novine.nn.hr/clanci/sluzbeni/2025_10_125_1785.html.

[17] Bulgakova, D. & Bulgakova, V. (2023) Realisation of the Right to Personal Data Protection in the Court of Justice of the European Union practice regardless of DIGITAL RIGHTS IRELAND, GOOGLE SPAIN, SCHREMS, TELE2 rulings. *Ukrainian Journal of International Law, 1,* 53-62. http://dx.doi.org/10.36952/uail.2023.1.53-62.

Дар'я Анатоліївна Булгакова
адвокат, доктор філософії з міжнародного права
доцент кафедри права та публічного управління
Запорізький інститут економіки та інформаційних технологій
50007, вул. Гетьманська, 108, Кривий Ріг, Україна
e-mail: dariabulgakova@yahoo.com
ORCID 0000-0002-8640-3622

Daria A. Bulgakova
An Advocate, Ph.D. in International Law
Associate Professor
Department of Law and Public Administration
Zaporizhzhia Institute of Economics and Information Technologies
50007, 108 Hetmanska Str., Kryvyi Rih, Ukraine
e-mail: dariabulgakova@yahoo.com
ORCID 0000-0002-8640-3622

Рекомендоване цитування: Булгакова Д. А. Ідентифікація без надмірності у метавсесвіті: баланс між публічним інтересом і вимогами GDPR. *Проблеми законності*. 2026. Вип. 172. С. 324–348. https://doi.org/10.21564/2414-990X.172.353393.

Suggested Citation: Bulgakova D.A. (2026). Identification Without Redundancy in the Metaverse: Balance between Public Interest and GDPR Requirements. *Problems of Legality, 172,* 324-348. https://doi.org/10.21564/2414-990X.172.353393.

Статтю подано / Submitted: 10.02.2026
Доопрацьовано / Revised: 15.03.2026
Схвалено до друку / Accepted: 25.03.2026
Опубліковано / Published: 31.03.2026