

UWARUNKOWANIA PRAWNE ZASTOSOWANIA I ROZWOJU METAVERSE W MEDYCYNIE

ADAM KOZIEN^{*}

DOI: 10.26399/iusnovum.v19.2.2025.18/a.kozien

STRESZCZENIE

W artykule podjęto się analizy stopniowo rozwijającej się sfery *metaverse*, będącej współcześnie w pewnym sensie połączeniem rozwoju technologicznego ze światem Internetu oraz sztuczną inteligencją, z perspektywy uwarunkowań prawnych mających istotne dla medycyny znaczenie. Poruszono oryginalną problematykę tyżącą się sfery nowych wyzwań, przed jakimi stoi prawo w świecie postępującej cyfryzacji; równocześnie opracowanie to ma charakter przeglądowy i monograficzny. Jako tezę przyjęto, iż przy stosowaniu *metaverse* w medycynie może dochodzić do niebezpieczeństwa naruszenia praw i wolności człowieka, szczególnie w sferze wolności jednostki, ochrony danych osobowych oraz ochrony dóbr osobistych, co jest relewantne z perspektywy prawnej. Celem przeprowadzonych badań była prawna analiza *metaverse* zastosowanego do medycyny, a także identyfikacja niebezpieczeństw *metaverse* w kontekście niebezpieczeństwa naruszania podstawowych praw i wolności jednostki, oraz wskazanie w tym zakresie postulatów ustawodawczych. Analiza przedmiotu badań oraz jej wyniki mają charakter oryginalny, a swoim zasięgiem obejmują nie tylko prawo polskie, ale również międzynarodowe. Zastosowanie badań może mieć znaczenie nie tylko dla nauki, lecz też praktyki prawa, szczególnie w zakresie działań ustawodawczych na poziomie międzynarodowym, unijnym oraz krajowym.

Słowa kluczowe: prawo, *metaverse*, medycyna, ochrona danych osobowych, ochrona dóbr osobistych

^{*} dr, MBA, Katedra Postępowania Administracyjnego, Wydział Prawa i Administracji, Uniwersytet Jagielloński w Krakowie (Polska), e-mail: a.kozien@uj.edu.pl, ORCID: 0000-0002-9301-9645



Artykuł opublikowany w formule otwartego dostępu (open access) na licencji Uznanie autorstwa-Użycie niekomercyjne-Na tych samych warunkach 4.0 Międzynarodowe (CC BY-NC-SA 4.0) (<https://creativecommons.org/licenses/by-nc-sa/4.0/>).

LEGAL FRAMEWORKS FOR THE APPLICATION AND DEVELOPMENT OF THE METAVERSE IN MEDICINE

ABSTRACT

In the article titled "Legal Frameworks for the Application and Development of Metaverse in Medicine", an analysis is undertaken of the gradually evolving sphere of the metaverse. This sphere is currently, in a sense, a fusion of technological development with the world of the internet and artificial intelligence from the perspective of legal considerations crucial to medicine. The article addresses an original issue within the realm of new challenges faced by the law in the era of advancing digitization. Simultaneously, it has a review and monographic character. The central thesis posited is that the use of the metaverse in medicine may pose a danger of violating human rights and freedoms, particularly in the areas of individual liberty, personal data protection, and protection of personal rights, which is relevant from a legal standpoint. The aim of the conducted research was to analyze the application of the metaverse in medicine from a legal perspective and to identify the dangers of the metaverse in the context of the risk of infringing on fundamental rights and individual freedoms. Additionally, the study aims to propose legislative recommendations in this regard. The subject of the research and its results are original in nature, encompassing not only Polish law but also international law. The application of the research may be significant not only for academia but also for the practice of law, especially concerning legislative actions at the international, European Union, and national levels.

Key words: law, metaverse, medicine, personal data protection, protection of personal rights

WSTĘP

Współczesny świat rozwija się w sposób bardzo dynamiczny, szczególnie w zakresie nowoczesnych technologii. Obecnie jednak te aktualne technologie nie oznaczają wyłącznie ulepszenia technologicznego określonych urządzeń, czy też rozwoju Internetu, ale wiążą się również z wkraczającą stopniowo sztuczną inteligencją. Oprócz tego czymś całkowicie nowym, co może radykalnie zmienić sposób funkcjonowania ludzi, jest promowany obecnie – szczególnie przez media społecznościowe – *metaverse*: w pewnym sensie połączenie rozwoju technologicznego ze światem Internetu oraz sztuczną inteligencją. *Metaverse* należy traktować jako wirtualny nieograniczony świat (*metaversum*), który swoim zasięgiem obejmuje wszystkich ludzi, a w pewnym zakresie może nawet wykroczyć poza współczesne rozumienie świata i wszechświata. Idea *metaverse* jeszcze niedawno traktowana była w kategoriach hipotetycznych oraz *science fiction*. Dostrzec można jednak, że stopniowo koncepcje z gatunku *science fiction* pozbawiane są elementu *fiction* i stają się światem rzeczywistym, w którym jednostka musi się właściwie odnaleźć. Na tak zmieniający się świat nie można reagować wyłącznie w kategoriach zagrożenia albo zafascynowania, ale dostrzegając określone niebezpieczeństwa, starać się odpowiednio dostosowywać nowe zdobycze techniki i technologii, by służyły dobru jednostki oraz dobru wspólnemu. W tym zakresie ważnym elementem jest prawo powszechnie obowiązujące, które powinno stawiać określone wymogi oraz ramy formalne współczesnym zdobyczom technologicznym, tak by nie doprowadzić do

naruszenia praw i wolności jednostki określonych zarówno na poziomie prawa międzynarodowego, unijnego, jak i porządków krajowych demokratycznych państw prawa. *Metaverse* stopniowo pojawia się również w medycynie, gdzie z racji swojej specyfiki może w sposób szczególny ingerować w wolności i prawa jednostki.

METODYKA I METODOLOGIA BADAŃ

Celem przeprowadzonych badań była analiza z perspektywy prawnej *metaverse* w zastosowaniu do medycyny, a także identyfikacja niebezpieczeństw *metaverse* w kontekście niebezpieczeństwa naruszania podstawowych praw i wolności jednostki, a także wskazanie w tym zakresie postulatów ustawodawczych.

Podczas prowadzenia przedmiotowych badań zostały zastosowane następujące metody badawcze, charakterystyczne dla nauk prawnych:

- Metoda teoretyczno-prawna, w celu dokonania analizy pojęcia *metaverse* oraz instytucji prawnych mających relewantne znaczenie z perspektywy przedmiotowych badań.
- Metoda formalno-dogmatyczna, w celu dokonania analizy przepisów prawnych – źródeł prawa powszechnie obowiązującego pod kątem przedmiotu badań.
- Metoda krytyki piśmiennictwa, umożliwiająca dokonanie analizy w zakresie przedmiotu badań, a także wskazanie luk w obecnym stanie wiedzy oraz tendencji rozwojowych współczesnej nauki w zakresie tematu badań.

METaverse JAKO WSPÓŁCZESNE WYZWANIE TECHNOLOGICZNE

Metaverse jest obecnie jedną z bardziej dyskutowanych i rozwijanych technologicznie kwestii. *Metaverse*¹ jest związany z tworzoną aktualnie nową erą Internetu, wychodzącą poza obecnie przyjęte schematy technologiczne, ale również kulturowe i społeczne. Ta nowa era Internetu jest związana, po pierwsze, z zestawami w technologii VR (rzeczywistości wirtualnej) lub AR (rzeczywistości rozszerzonej), a po drugie, z tworzeniem oraz współistnieniem wielu wirtualnych światów cyfrowych 3D, a także wirtualnej rzeczywistości. Pojęcie „Metaverse” zostało utworzone przez Neala Stephensona w powieści science fiction *Snow Crash* z 1992 roku, gdzie jest nim wirtualny świat, funkcjonujący równolegle do świata rzeczywistego. Obecnie zwolennikiem i propagatorem *metaverse* jest Mark Zuckerberg, twórca Facebooka, który dostrzega przyszłość organizacji w *metaverse*. Aktualnie *metaverse* znajduje się w polu zainteresowania takich przedsiębiorstw, jak: Microsoft, Apple, Epic Games. Równocześnie istnieją obecnie platformy oparte na *metaverse*, jak: Fortnite oraz

¹ Zob. M. Sparkes, *What Is a Metaverse*, „New Scientist” 2021, Vol. 251, Iss. 3348; S. Mystakidis, *Metaverse*, „Encyclopedia” 2022, Vol. 2 (1); I.A. Filipova, *Creating the Metaverse: Consequences for Economy, Society, and Law*, „Journal of Digital Technologies and Law” 2023, Vol. 1 (1); M. Kalyvaki, *Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction*, „Journal of Metaverse” 2023, Vol. 3 (1); S. Kasiyanto, M.R. Kilinc, *The Legal Conundrums of the Metaverse*, „Journal of Central Banking Law and Institutions” 2022, Vol. 1 (2).

Roblox, które są związane z grami. Warto również zauważyć, że technologia VR umożliwia, oprócz poruszania się po świecie wirtualnym, także odczuwanie wrażeń zmysłowych, natomiast technologia AR, pobierając elementy ze świata *metaverse*, mapuje je następnie na rzeczywisty świat.

W tym kontekście warto wskazać, że obecnie sfera Internetu oraz mediów społecznościowych pozwala na wirtualne funkcjonowanie *metaverse*, jednakże nadal zachowany zostaje podział na sferę świata rzeczywistego oraz świata wirtualnego, nawet jeśli świat wirtualny staje się coraz bardziej podobny do świata rzeczywistego. Ideą *metaverse* jest utworzenie świata cyfrowego, który stałby się światem rzeczywistym. Co więcej, możliwe – z perspektywy technologicznej – jest istnienie kilku światów wirtualnych niezależnych lub wzajemnie nachodzących na siebie. Za pomocą *metaverse* możliwe będzie funkcjonowanie w świecie wirtualnym i w świecie rzeczywistym, a zatem nawiązywanie kontaktów z innymi osobami, załatwianie spraw, robienie zakupów, granie w gry, zwiedzanie różnych miejsc bez wychodzenia z domu. Co więcej, możliwe będzie również połączenie różnych wirtualnych światów, pomiędzy którymi można się swobodnie poruszać, posiadając odpowiedni sprzęt techniczny. Ważnym aspektem *metaverse* jest też fakt, iż osoba wchodząca w wirtualny świat czuje, jakby w nim się rzeczywiście poruszała i funkcjonowała. Powoduje to niebezpieczeństwo zacierania się światów wirtualnego i rzeczywistego.

Aby możliwe było funkcjonowanie w świecie *metaverse*, konieczne jest tworzenie awatarów² konkretnych osób, za pomocą których można się poruszać po świecie *metaverse* jak w świecie rzeczywistym i być również rozpoznawanym przez innych użytkowników. W świecie *metaverse*, w którym z założenia można funkcjonować jak w świecie rzeczywistym, należy również wprowadzić wirtualną własność mienia, towarów i tożsamości, konieczne jest wprowadzenie odpowiedniej struktury nie tylko technologicznej, ale również ekonomicznej. W tym celu są tam kryptowaluty oraz niewymienialne tokeny (*non-fungible token* – NFT).

Istnienie wirtualnych światów *metaverse* związane jest silnie z funkcjonowaniem sztucznej inteligencji. *Metaverse* ma charakter świata wirtualnego, cyfrowego, który opiera się na systemach teleinformatycznych, a w nich, stopniowo, coraz większą rolę odgrywa sztuczna inteligencja. Na ten moment sztuczna inteligencja działa na podstawie oprogramowania tworzonego i kontrolowanego przez człowieka. Jednak rozważyć należy w niedalekiej przyszłości istnienie sieci neuronowych, które będą mogły same od siebie się uczyć, rozwijać i myśleć – niezależnie od zaprogramowania przez człowieka. Powstaje zatem futurologiczne pytanie: czy w pewnym momencie samoucząca się i samomyśląca sztuczna inteligencja nie zacznie niezależnie od człowieka rządzić wirtualnym światem *metaverse*? Obecnie jest to pytanie całkowicie futurologiczne, ale równocześnie, gdyby zadać dekadę temu pytanie o tworzenie wirtualnych światów *metaverse*, odbiór w opinii publicznej również miałby charakter całkowicie futurologiczny i nierealny.

² B.C. Cheong, *Avatars in the Metaverse: Potential Legal Issues and Remedies*, „International Cybersecurity Law Review” 2022, Vol. 3.

METAVERSE W MEDYCYNIE

Metaverse może znaleźć również zastosowanie w obszarze nauk przyrodniczych³, w tym również w medycynie. Świat 3.0 otwiera tu nowe możliwości⁴. Z uwagi na fakt, że *metaverse* przybliża się coraz bardziej do świata rzeczywistego, może być on bardzo pomocny w medycynie. Przykładem zastosowania *metaverse* w medycynie mogą być konsultacje lub nawet leczenie w świecie *metaverse* za pośrednictwem awatarów. W takim przypadku awatar pacjenta posiadałby pełną dokumentację medyczną rzeczywistego pacjenta i na tej podstawie lekarz mógłby prowadzić konsultację medyczną. Oczywiście, nie wszystkie badania byłby możliwe do przeprowadzenia w świecie *metaverse*, ale konsultacje, jak porady np. żywieniowe lub też ogólnie pojmowana telemedycyna, są możliwe do przeprowadzenia w wirtualnym świecie. Tego typu konsultacje medyczne wyeliminowałyby również bariery geograficzne oraz społeczne.

Warto również zauważyć, że medyczny świat *metaverse* mógłby znacząco pomóc w kształceniu przyszłych lekarzy, ponieważ pozwalałby na przeprowadzanie nieinwazyjnych badań i porad w świecie wirtualnym, a także mógłby być przydatny w symulowaniu, przykładowo, prawdziwej operacji chirurgicznej. Podkreślenia wymaga fakt, że istnieją obecnie projekty utworzenia placówki medycznej w *metaverse*, a także założenie szpitala *metaverse* w Zjednoczonych Emiratach Arabskich. Dostrzegalny jest również potencjał tzw. cyfrowych bliźniaków, czyli wirtualnych modeli rzeczywistych istot lub obiektów.

Korzyści z *metaverse* dostrzegają również przedsiębiorstwa farmaceutyczne, które inwestują w badania kliniczne. Kolejną kwestią są również dane pacjentów, cenne z perspektywy badań w naukach przyrodniczych oraz opiece zdrowotnej. Obecnie pacjenci za przekazanie swoich danych zazwyczaj nie otrzymują wynagrodzenia. W świecie *metaverse* tokeny NFT umożliwiłyby kodowanie, a następnie przenoszenie własności i wartości danych. W konsekwencji pacjenci mogliby zarabiać na swoich danych i decydować, komu je udostępnić jako NFT.

Rozwój *metaverse* w medycynie związany jest z presją regulacyjną, znaczącymi niedoborami w personelu medycznym, a także zmianą podejścia w kierunku zwiększonego budowania zaufania do pacjenta z uwagi na fakt podejmowania przez niego licznych decyzji. Jako pierwsze podstawowe obszary aplikacji *metaverse* w naukach medycznych można wskazać edukację oraz szkolenia. Warto zauważyć, że wizualizacje 3D umożliwiają rzeczywiste rozwijanie oraz podnoszenie kwalifikacji personelu medycznego bez szkody dla pacjentów. Szkolenia te również możliwe są niezależnie od barier geograficznych, środowiskowych i kulturowych. Symulacje

³ Zob. S. Surveswaran, L. Deshpande, *A Glimpse into the Future: AI, Digital Humans, and the Metaverse – Opportunities and Challenges for Life Sciences in Immersive Ecologies*, w: M. Byrne (red.), *AI in Clinical Medicine: A Practical Guide for Healthcare Professionals*, Wiley-Blackwell, 2023.

⁴ Zob. też: <https://www.cognizant.com/us/en/insights/perspectives/in-life-sciences-the-metaverse-opportunity-knocks-wf1135812> (dostęp: 20.05.2023); https://www.ey.com/en_ch/technology/how-can-life-sciences-and-healthcare-thrive-in-the-metaverse (dostęp: 20.05.2023); <https://www.tcs.com/what-we-do/industries/life-sciences/white-paper/metaverse-healthcare-life-sciences-realize-business-value> (dostęp: 20.05.2023).

często związane są z grywalizacją, która odbywa się w tym przypadku bez ryzyka. Zaawansowanie technologiczne symulacji pozwala na zaangażowanie wszystkich zmysłów osoby szkolonej i pozwala wytworzyć rzeczywiste odczucia i doświadczenia. Szkolenie medyczne może być prowadzone dla pracowników służby zdrowia, ale też dla farmaceutów w zakresie wizualizacji działania leku; istotne jest symulowanie doświadczeń wynikających ze zróżnicowanych warunków danej osoby. Współcześnie uniwersytety medyczne szkolą studentów przy wykorzystaniu *metaverse* przykładowo w wirtualnej sali operacyjnej z wirtualnym pacjentem.

Kolejnym przykładem wprowadzenia *metaverse* w medycynie jest zmiana w badaniach klinicznych, ponieważ *metaverse* – dzięki temu, że brak tu ograniczeń zarówno geograficznych, jak i fizycznych – może uczynić te badania bardziej zdecentralizowanymi i możliwymi do przeprowadzenia w domach pacjentów. Celem zapewnienia w tym zakresie bezpieczeństwa i ochrony danych pacjentów ważnym elementem powinny pozostać NFT, przykładowo w perspektywie dokumentacji medycznej. *Metaverse* może również umożliwić tak zwane immersyjne terapie, a zatem interwencje medyczne za pomocą AR, VR i MR. W sposób szczególny może to znaleźć zastosowanie przy terapiach poznawczych, rehabilitacji, a także leczeniu psychiatrycznym oraz psychologicznym. *Metaverse* może zostać również zastosowany przy diagnostyce radiologicznej, ponieważ obecnie obrazy medyczne wizualizowane są na ekranach 2D. Ulepszenie diagnostyki w 3D umożliwi lepszą analizę obrazu medycznego, a także pozwoli na zastosowanie interaktywnych oraz realistycznych doświadczeń medycznych. W tym zakresie pojawiają się obecnie sprzęty medyczne, które z użyciem VR szkolą robotę medycznego z wykorzystaniem algorytmów uczenia maszynowego.

Metaverse może też przyczynić się do rozwoju telemedycyny – to szczególnie ważne z uwagi na braki kadrowe oraz technologiczne w służbie zdrowia. W tym zakresie istotne stają się: rozszerzona rzeczywistość i świadczenie usług medycznych, jak diagnostyka, konsultacje, leczenie, opieka oraz monitorowanie w formie zdalnej. W konsekwencji również ważne znaczenie mogą mieć tzw. cyfrowe bliźniaki, które umożliwią dokonywanie symulacji w formie trójwymiarowej.

PROBLEMY I WYZWANIA PRAWNE W ZAKRESIE ZASTOSOWANIA METAVERSE W ODNIESIENIU DO MEDYCYNY

WOLNOŚĆ JEDNOSTKI W PERSPEKTYWIE ZASTOSOWANIA METAVERSE W MEDYCYNIE

Jako pierwszą kwestię można wskazać niebezpieczeństwo naruszenia wolności oraz praw człowieka. Zaznaczyć należy, że wolność jest powiązana z samą naturą człowieka, przez co nie jest ona określana przez państwo, natomiast ma charakter pierwotny⁵. Wolność jednostki polega na tym, że ma ona prawo, w konkretnej sytuacji, dokonać wyboru lub też czynności zgodnie z własną wolą, pod warunkiem, że nie

⁵ B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej*, Warszawa 2012, s. 201.

są one prawem zabronionym⁶. Wolność człowieka nie wynika z „prawa w znaczeniu przedmiotowym, a prawo jedynie ustanawia jej granice”⁷. Należy również zaznaczyć za L. Garlickim, że zasada wolności „jest to jedna z typowych metanorm (klausul generalnych) określających sposób i kierunek interpretacji całego systemu norm konstytucyjnych oraz wyznaczająca system wartości, któremu system ten ma służyć”⁸.

Należy zatem rozważyć, kto w *metaverse* będzie czuwał nad przestrzeganiem wolności i praw człowieka, zwłaszcza że *metaverse* z założenia ma charakter globalny oraz ponadpaństwowy i ponadnarodowy, czyli również jaki porządek prawny będzie obowiązujący⁹.

Dużym zagrożeniem dla wolności jednostki w *metaverse* może być nierównorzędnność występująca pomiędzy administratorami *metaverse* a jednostkami chcącymi rozpocząć korzystanie oraz korzystającymi z usług *metaverse*. Ta nierównorzędnność wynika w sposób szczególny z pozycji i siły podmiotów administrujących *metaverse*. Aby było możliwe korzystanie z *metaverse*, konieczne jest zawarcie odpowiedniej umowy, która w zasadzie ma charakter adhezyjny, co może prowadzić do naruszeń autonomii woli oraz wolności jednostki.

Niebezpieczeństwa można zauważyć nie tylko w prywatnoprawnej relacji wertykalnej pomiędzy administratorem *metaverse* a użytkownikiem, ale również w prywatnoprawnej relacji horyzontalnej pomiędzy poszczególnymi jednostkami, korzystającymi z danego *metaverse*, szczególnie w zakresie dóbr osobistych. Istotnym elementem może być również relacja między państwem a danym *metaverse*, a także fakt, czy w świecie *metaverse* będą występowały państwa.

Zagrożenia wolności jednostki w *metaverse* mogą dotyczyć również ochrony danych osobowych, stosunków zobowiązaniowych pomiędzy administratorami *metaverse* a ich użytkownikami, prawnoautorskich, karnoprawnych, prawno międzynarodowych.

Ponadto zagrożenia wolności jednostki w *metaverse* mogą pojawić się również ze strony nowych technologii, a szczególnie tzw. „sztucznej inteligencji” oraz systemów informatycznych. Wspomnieć należy również o niebezpieczeństwie naruszenia zasady równości oraz niedyskryminacji, szczególnie w kontekście tak zwanego „wykluczenia cyfrowego”, szczególnie osób starszych, biednych, mieszkających na terenach mało zurbanizowanych, gdzie dostęp do sieci internetowej bywa znacząco utrudniony albo w ogóle niemożliwy. Powstaje również strategiczne pytanie: kto może być użytkownikiem *metaverse*, szczególnie w perspektywie osób z ograniczoną zdolnością do czynności prawnych lub osób z jej brakiem. W tym zakresie wskazać należy, że przy ocenie realizacji zasady równości należy odwoływać się do niej w znaczeniu materialnym. W tym kontekście polski Trybunał Konstytucyjny zaznaczył, że:

⁶ W. Skrzydło, S. Grabowska, R. Grabowski, *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, Warszawa 2009, s. 643.

⁷ B. Banaszak, *Konstytucja...*, op. cit., s. 202.

⁸ L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2012, s. 94.

⁹ Zob. też: M. Turdialiev, *Legal Discussion of Metaverse Law*, „International Journal of Cyber Law” 2023, Vol. 1 (3).

Sprawą podstawową dla oceny dochowania zasady równości jest tym samym ustalenie cechy istotnej, z uwagi na którą przepisy prawa dokonały zróżnicowania sytuacji prawnej swoich adresatów. (...) Wielokrotnie wskazywano więc, że różnicowanie sytuacji prawnej obywateli jest wtedy sprzeczne z konstytucją, jeżeli traktuje się w sposób różny podmioty lub sytuacje podobne, a takie różnice traktowania nie znajdują należytego uzasadnienia konstytucyjnego. Trybunał Konstytucyjny wielokrotnie podkreślał również związek zasady równości z zasadą sprawiedliwości (...)¹⁰.

W poszukiwaniu takiego uzasadnienia wskazywano kryteria racjonalności, proporcjonalności i sprawiedliwości dokonywanych zróżnicowań (...)¹¹. Innymi słowy, wszelkie odstępstwa od nakazu równego traktowania podmiotów podobnych muszą zawsze znajdować podstawę w odpowiednio przekonywujących kryteriach. Kryteria te muszą mieć:

- po pierwsze, charakter relewantny, a więc pozostawać w bezpośrednim związku z celem i zasadniczą treścią przepisów, w których zawarta jest kontrolowana norma oraz służyć realizacji tego celu i treści, czyli wprowadzane zróżnicowania muszą mieć charakter racjonalnie uzasadniony. Nie wolno ich dokonywać według dowolnie ustalonego kryterium (...)¹²;
- po drugie, charakter proporcjonalny, a więc waga interesu, któremu ma służyć różnicowanie sytuacji adresatów normy, musi pozostawać w odpowiedniej proporcji do wagi interesów, które zostaną naruszone w wyniku nierównego potraktowania podmiotów podobnych;
- po trzecie, muszą pozostawać w jakimś związku z innymi wartościami, zasadami czy normami konstytucyjnymi, uzasadniającymi odmienne traktowanie podmiotów podobnych (...)¹³ (...)¹⁴.

W konsekwencji zatem pewien zakres zróżnicowania może występować, ale musi on zależeć od zobiektywizowanych kryteriów i nie może prowadzić przykładowo do „wykluczenia cyfrowego”.

OCHRONA DANYCH OSOBOWYCH W PERSPEKTYWIE ZASTOSOWANIA METAVERSE W MEDYCYNIE

Ważnym wyzwaniem prawnym jest kwestia ochrony danych osobowych w *metaverse*. W tym zakresie problematycznymi kwestiami są liczba i zakres danych osobowych, które będą umieszczane w przestrzeni *metaverse*. Początki regulacji prawnych,

¹⁰ Orzeczenie Trybunału Konstytucyjnego z dnia 28.11.1995 r., sygn. K. 1/95, OTK ZU Nr 3/1995, s. 183.

¹¹ Orzeczenie Trybunału Konstytucyjnego z dnia 3.09.1996 r., sygn. K. 10/96, OTK ZU Nr 5/1996, s. 281.

¹² Orzeczenie Trybunału Konstytucyjnego z dnia 12.12.1994 r., sygn. K. 3/94, OTK w 1994 r., cz. II, s. 141.

¹³ Przykładowo np. Orzeczenie Trybunału Konstytucyjnego z dnia 23.10.1995 r., sygn. K. 4/95, OTK w 1995 r., cz. II, s. 93.

¹⁴ Wyrok Trybunału Konstytucyjnego z dnia 16.12.1997 r., sygn. K 8/97, OTK 1997, nr 5–6, poz. 70. Zob. także: Wyrok Sądu Najwyższego z dnia 5.05.2010 r., sygn. I PK 201/09.

związanych z kwestią danych osobowych, można dostrzec w latach 70. XX wieku¹⁵, jednak wtedy kwestię tę ujmowano na dwa sposoby – poprzez tworzenie regulacji fragmentarycznych i kompleksowych (dla przykładu można wskazać ustawę o ochronie danych osobowych z 1970 r. landu niemieckiego Hesja)¹⁶. Konieczność rozbudowywania i poszerzania ochrony danych osobowych była związana z trwającą informatyzacją różnych dziedzin życia i tworzeniem skomputeryzowanych systemów¹⁷, mogących zapisywać, a także przetwarzać, liczne dane, a w konsekwencji – z pojawianiem się *de facto* baz danych¹⁸. Brak adekwatnej odpowiedzi prawnej doprowadziłby do nieograniczonego gromadzenia oraz przetwarzania danych osobowych. W rezultacie stwarzałoby to niebezpieczeństwo naruszenia nie tylko prawa do prywatności, ale również samej istoty wolności i praw człowieka¹⁹.

Prawna ochrona danych osobowych występuje na gruncie prawa międzynarodowego, unijnego oraz poszczególnych krajów, ale wśród tych regulacji warto wspomnieć o Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)²⁰, które w sposób holistyczny chroni dane osobowe na terenie państw członkowskich Unii Europejskiej. Wprowadzenie Rozporządzenia pozwoliło na pełną harmonizację na terenie Unii Europejskiej ochrony danych osobowych. Warto zaznaczyć, że Rozporządzenie nie odnosi się wyłącznie do państw członkowskich Unii Europejskiej, ale swoim zasięgiem dotyczy również podmiotów, które świadczą usługi na terenie Unii Europejskiej²¹. Na podstawie art. 3 ust. 1 Rozporządzenia ma ono zastosowanie „do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii”, a art. 3 ust. 2 stanowi, iż Rozporządzenie ma zastosowanie „do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

- a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
- b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii”.

¹⁵ J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, s. 25.

¹⁶ Ibidem, s. 25; W. Kilian, *Ochrona danych w przedsiębiorstwach*, w: M. Wyrzykowski (red.), *Ochrona danych osobowych (zbiór referatów wygłoszonych na poświęconej problematyce ochrony danych osobowych konferencji naukowej w dniach 27–28 II 1998 r.)*, Warszawa 1999, s. 99 i n.

¹⁷ J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych...*, op. cit., s. 26.

¹⁸ Zob. też U. Seidel, *Datenbanken und Persönlichkeitsrecht*, Köln 1972.

¹⁹ J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych...*, op. cit., s. 27.

²⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119/1 z 4.05.2016.

²¹ M. Krawczyk, *Ochrona danych osobowych w Internecie*, w: A. Surma, E. Chodźko (red.), *Współczesne wyzwania cyfryzacji – przegląd i badania*, Lublin 2019, s. 190.

Traktując *metaverse* jako rzeczywisty świat w przestrzeni wirtualnej, można dojść do sytuacji, w której w zasadzie wszystkie dane o danej jednostce będą przechowywane i przetwarzane w świecie *metaverse*. Część z tych danych będzie zapewne podawana obligatoryjnie, a część fakultatywnie. Konieczne jest zatem maksymalne zminimalizowanie liczby danych podawanych obligatoryjnie, ponieważ co do danych podawanych fakultatywnie można stosować zasadę *volenti non fit iniuria*.

Problemem ponadto będą dane, które nie będą umieszczane świadomie i bezpośrednio, oraz te, które będą przekazywane w sposób nieświadomy i pośredni, zazwyczaj w wyniku umieszczania danych świadomie i w sposób bezpośredni. W zakresie ochrony danych osobowych ponownie ważnym elementem będzie prawo właściwe, zwłaszcza że, przykładowo, regulacje unijne są w tym zakresie bardzo restrykcyjne, w przeciwieństwie do innych porządków prawnych. Zaznaczyć również należy, że obecnie dane osobowe są współczesnym towarem i z perspektywy administratorów *metaverse*, a także podmiotów prowadzących tam działalność gospodarczą, mają znaczenie oraz są cenne (mają wartość policzalną). Kolejnym problemem są również tak zwane metadane, powstające w wyniku działalności konkretnego użytkownika. Administratorzy *metaverse* mogą również pobierać dane z oprogramowania użytkownika.

Niebezpieczeństwo naruszenia ochrony danych osobowych nie pochodzi jedynie ze strony administratorów *metaverse* gromadzących i przetwarzających dane, ale również ze strony innych użytkowników portali społecznościowych, a nawet przestępców działających w zakresie cyberprzestępczości. Wskazać należy, że w medycynie mamy do czynienia z danymi osobowymi szczególnie wrażliwymi, bo przykładowo dotyczącymi stanu zdrowia, więc tym bardziej ochrona powinna być posunięta maksymalnie daleko. Należy też zauważyć, że świat *metaverse* będzie przetwarzał i gromadził ogromne liczby danych, które wykrócą nawet poza rozumienie tak zwanych big data²² – a obecnie to ono dominuje w sferze Internetu i mediów społecznościowych.

OCHRONA DÓBR OSOBISTYCH W PERSPEKTYWIE ZASTOSOWANIA METAVERSE W MEDYCYNIE

Wyzwaniem jest również ochrona dóbr osobistych. W ujęciu szerszym nie bezpośrednio do *metaverse*, ale do kwestii naruszenia dóbr osobistych w Internecie można wskazać następujące poglądy w doktrynie prawniczej:

²² Zob. D. Boyd, K. Crawford, *Critical Questions For Big Data in Information*, „Communication & Society” 2012, Vol. 15, Iss. 5, s. 662–679; H.U. Buhl, M. Röglinger, F. Moser, J. Heidemann, *Big Data. Ein (ir-)relevanter Modebegriff für Wissenschaft und Praxis?*, „Wirtschaftsinformatik” 2013, Vol. 55, Iss. 2, s. 63–68; R. Reichert, *Big Data*, w: T. Beyes, J. Metelmann, C. Pias (Hrsg.), *Nach der Revolution. Ein Brevier digitaler Kulturen*, Berlin 2017, s. 177–185; M. Schermann, H. Krcmar, H. Hensen, V. Markl, Ch. Buchmüller, T. Bitter, T. Hoeren, *Big Data – An Interdisciplinary Opportunity for Information Systems Research*, „Business & Information Systems Engineering” 2014, Vol. 6, Iss. 5, s. 261–266; D. Klein, P. Tran-Gia, M. Hartmann, *Big Data*, „Informatik Spektrum” 2013, Vol. 36, s. 319–323; V. Marx, *The Big Challenges of Big Data*, „Nature” 2013, Vol. 498, s. 255–260.

- można dokonać podziału na dobra osobiste, które mogą zostać naruszone lub zagrożone w Internecie²³;
- istnieją dobra osobiste, które mogą zostać naruszone lub zagrożone tylko w świecie rzeczywistym – np. nietykalność mieszkania²⁴;
- w zasadzie wszystkie dobra osobiste mogą być naruszone lub zagrożone w Internecie²⁵.

Biorąc pod uwagę *metaverse*, wskazać należy, że każde dobro osobiste może co do zasady zostać tam naruszone lub też zagrożone. Problematyka ochrony dóbr osobistych w prawie powszechnie obowiązującym ma charakter norm ogólnych, otwartego katalogu dóbr prawnie chronionych i podatnych na dynamicznie zmieniające się okoliczności w życiu politycznym, prawnym, społecznym, gospodarczym oraz kulturowym.

Znaczącym wyzwaniem dla dóbr osobistych w perspektywie *metaverse* jest ich globalny charakter, co może znacząco osłabić efektywność dochodzenia swoich praw i roszczeń i powoduje konieczność wypracowania na poziomie międzynarodowym skutecznych mechanizmów dochodzenia roszczeń. W tym zakresie naprzeciw może wyjść również sądownictwo internetowe, które jest już znane przykładowo w Chinach.

Specyfika *metaverse* powoduje, iż poza tradycyjnymi formami naruszania dóbr osobistych, takich jak np. obrażanie, zamieszczanie kompromitujących zdjęć innych osób, pisanie nieprawdy odnośnie do innych, bezprawne wykorzystywanie czyjegoś nazwiska, twórczości, można wskazać inne formy naruszania dóbr osobistych, do których można zaliczyć: *spamming*, *cookies*²⁶, retencję danych, tworzenie profili osobowościowych, *phishing*²⁷, ataki hakerskie²⁸, podszywanie się pod dany podmiot, *sniffing*, *heartbleed bug*, *deep links*, *cloud computing*. Specyfika *metaverse* może prowadzić do dokonywania naruszeń tych samych dóbr osobistych, tylko w innych formach (specyficznych dla przestrzeni wirtualnej), a także do powstawania nowych form naruszeń dóbr osobistych. Co do zasady, każde dobro osobiste może zostać naruszone w *metaverse*. Naruszenia te mogą zostać dokonane zarówno przez podmioty prawa publicznego, jak i przez podmioty prawa prywatnego, a szczególnie przez administratorów oraz użytkowników *metaverse*. Naruszenia mogą być dokonywane w sytuacji ataków hakerskich lub też włamania się na konto użytkownika

²³ P. Modrzejewski, *Sposoby naruszania dóbr osobistych w Internecie – zagadnienia wybrane*, „Studia Prawnoustrojowe” 2019, nr 44, s. 295; J. Sadowski, *Naruszenie dóbr osobistych przez media*, Warszawa 2003, s. 26.

²⁴ P. Modrzejewski, *Sposoby naruszania dóbr osobistych w Internecie – zagadnienia wybrane*, „Studia Prawnoustrojowe” 2019, nr 44, s. 295–296. Zob. P. Wąglowski, *Ochrona dóbr osobistych i danych osobowych*, Warszawa 2009, s. 4.

²⁵ P. Wąglowski, *Ochrona dóbr osobistych i danych osobowych*, Warszawa 2009, s. 4–5; P. Modrzejewski, *Sposoby naruszania dóbr osobistych w Internecie – zagadnienia wybrane*, „Studia Prawnoustrojowe” 2019, nr 44, s. 296.

²⁶ M.R. Siebecker, *Cookies and the Common Law: Are Internet Advertisers Trespassing On Our Computers?*, „Southern California Law Review” 2003, Vol. 76 (4).

²⁷ J.A. Chaudhry, S.A. Chaudhry, R.G. Rittenhouse, *Phishing Attacks and Defenses*, „International Journal of Security and Its Applications” 2016, Vol. 10, No. 1.

²⁸ K. Anderson, *Hacktivism and Politically Motivated Computer Crime*, Portland 2008; M.T. Simpson, *Hands-on Ethical Hacking and Network Defense*, Boston 2013.

portalu społecznościowego przez osobę nieuprawnioną. Współcześnie do naruszenia dóbr osobistych może również dochodzić w wyniku działania systemów informatycznych sterowanych przez osoby fizyczne, ale także poprzez działalność AI.

Jednym z ważniejszych wyzwań jest zapewnienie bezpieczeństwa w świecie *metaverse*, szczególnie bezpieczeństwa danych, ponieważ to one będą miały szczególne znaczenie w wirtualnym świecie. Bezpieczeństwo techniczne powinno zabezpieczać przed atakami hakerskimi i szeroko pojętą cyberprzestępczością. Szczególnie należy zwrócić uwagę na bezpieczeństwo danych zarówno wrażliwych, jak i tych dotyczących stanu zdrowia.

PODSUMOWANIE

Idea *metaverse* całkowicie zmienia podejście do funkcjonowania w przestrzeni wirtualnej. Sam pomysł istnienia równoległych światów wirtualnych, które w zasadzie są powieleniem świata rzeczywistego, wydaje się nadal abstrakcyjny, jednakże jest w zasadzie w części dostępny. Istnienie świata *metaverse* można dostrzec w różnych dziedzinach życia, w tym w naukach przyrodniczych, a tu w sposób szczególny w medycynie oraz naukach o zdrowiu. Rodzi to duże wyzwania w zakresie prawnym, ponieważ świat *metaverse* funkcjonuje równolegle do świata rzeczywistego, a zatem podstawowym problemem jest określenie prawa właściwego. Kolejną kwestią jest niebezpieczeństwo naruszenia praw oraz wolności jednostki, które może wynikać z dominującej pozycji administratorów *metaverse*, a także z niebezpieczeństwa tak zwanego „wykluczenia cyfrowego”. Ważnymi elementami są: kwestia bezpieczeństwa cyfrowego w dobie cyberprzestępczości i kwestia ochrony danych osobowych i dóbr osobistych oraz roli sztucznej inteligencji. Dostosowanie prawa w tym zakresie dotyczy nie tylko prawa międzynarodowego czy też cywilnego, ale również administracyjnego, karnego, gospodarczego oraz unijnego.

Wskazane powyżej niebezpieczeństwa są tylko tymi najbardziej jaskrawymi, szczególnie w perspektywie medycyny. Niezależnie od faktu, że problematyka ta ma charakter międzynarodowy, ostatecznie z tymi problemami będzie musiał sobie poradzić ustawodawca krajowy. Państwo jako aparat administracyjny ma relatywnie szerokie uprawnienia do zaingerowania w tę działalność, lecz równocześnie musi pamiętać o konieczności zachowania przy tym proporcjonalności, a także respektowania wolności i praw jednostki. Niezależnie od perspektywy publiczno-prawnej, a zatem administracyjnej i karnistycznej, ważnym elementem powinna być również ingerencja na poziomie cywilnoprawnym poprzez chociażby wprowadzenie specyficznej umowy dotyczącej korzystania z usług w świecie *metaverse*, która chroniłaby użytkowników tej formy działania w sferze szeroko pojętego Internetu.

Niezależnie od powyższych rozważań, należy wskazać, iż konieczna jest w tym zakresie zmiana kultury, zwyczajów i podejścia społeczeństwa do świata wirtualnego. Jest to element, który będzie ewoluował przez pewien czas. Poza tym człowiek przez świat *metaverse* nie może zostać uzależniony od świata wirtualnego, który powinien jedynie pomagać w normalnym funkcjonowaniu. Świat wirtualny nigdy nie zastąpi świata rzeczywistego, ponieważ w najlepszym wypadku będzie

go tylko wiernie imitował. Wbrew pozorom bardzo dobrze pokazuje to przykład medycyny, bo przecież chirurg nie przeprowadzi operacji w świecie wirtualnym. Ponadto można zadać pytanie, czy wirtualny świat *metaverse* kiedykolwiek dorówna pięknu świata rzeczywistego?

BIBLIOGRAFIA

- Anderson K., *Hackivism and Politically Motivated Computer Crime*, Portland 2008.
- Banaszak B., *Konstytucja Rzeczypospolitej Polskiej*, Warszawa 2012.
- Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2011.
- Boyd D., Crawford K., *Critical Questions For Big Data in Information*, „Communication & Society” 2012, Vol. 15, Iss. 5.
- Buhl H.U., Röglinger M., Moser F., Heidemann J., *Big Data. Ein (ir-)relevanter Modebegriff für Wissenschaft und Praxis?*, „Wirtschaftsinformatik” 2013, Vol. 55, Iss. 2.
- Chaudhry J.A., Chaudhry S.A., Rittenhouse R.G., *Phishing Attacks and Defenses*, „International Journal of Security and Its Applications” 2016, Vol. 10, No. 1.
- Cheong B.C., *Avatars in the Metaverse: Potential Legal Issues and Remedies*, „International Cyber-security Law Review” 2022, Vol. 3.
- Filipova I.A., *Creating the Metaverse: Consequences for Economy, Society, and Law*, „Journal of Digital Technologies and Law” 2023, Vol. 1 (1).
- Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2012.
- Kalyvaki M., *Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction*, „Journal of Metaverse” 2023, Vol. 3 (1).
- Kasiyanto S., Kilinc M.R., *The Legal Conundrums of the Metaverse*, „Journal of Central Banking Law and Institutions” 2022, Vol. 1 (2).
- Kilian W., *Ochrona danych w przedsiębiorstwach*, w: M. Wyrzykowski (red.), *Ochrona danych osobowych (zbiór referatów wygłoszonych na poświęconej problematyce ochrony danych osobowych konferencji naukowej w dniach 27–28 II 1998 r.)*, Warszawa 1999.
- Klein D., Tran-Gia P., Hartmann M., *Big Data*, „Informatik Spektrum” 2013, Vol. 36.
- Krawczyk M., *Ochrona danych osobowych w Internecie*, w: A. Surma, E. Chodźko (red.), *Współczesne wyzwania cyfryzacji – przegląd i badania*, Lublin 2019.
- Marx V., *The Big Challenges of Big Data*, „Nature” 2013, Vol. 498.
- Modrzejewski P., *Sposoby naruszania dóbr osobistych w Internecie – zagadnienia wybrane*, „Studia Prawnoustrojowe” 2019, nr 44.
- Mystakidis S., *Metaverse*, „Encyclopedia” 2022, Vol. 2 (1).
- Reichert R., *Big Data*, w: Beyes T., Metelmann J., Pias C. (Hrsg.), *Nach der Revolution. Ein Brevier digitaler Kulturen*, Berlin 2017.
- Schermann M., Krcmar H., Hensen H., Markl V., Buchmüller Ch., Bitter T., Hoeren T., *Big Data – An Interdisciplinary Opportunity for Information Systems Research*, „Business & Information Systems Engineering” 2014, Vol. 6, Iss. 5.
- Seidel U., *Datenbanken und Persönlichkeitsrecht*, Köln 1972.
- Siebeck M.R., *Cookies and the Common Law: Are Internet Advertisers Trespassing On Our Computers?*, „Southern California Law Review” 2003, Vol. 76 (4).
- Simpson M.T., *Hands-on Ethical Hacking and Network Defense*, Boston 2013.
- Skrzydło W., Grabowska S., Grabowski R., *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny*, Warszawa 2009.
- Sparkes M., *What Is a Metaverse*, „New Scientist” 2021, Vol. 251, Iss. 3348.

- Surveswaran S., Deshpande L., *A Glimpse into the Future: AI, Digital Humans, and the Metaverse – Opportunities and Challenges for Life Sciences in Immersive Ecologies*, w: M. Byrne (red.), *AI in Clinical Medicine: A Practical Guide for Healthcare Professionals*, Wiley-Blackwell, 2023.
- Turdialiev M., *Legal Discussion of Metaverse Law*, „International Journal of Cyber Law” 2023, Vol. 1 (3).
- Wagłowski P., *Ochrona dóbr osobistych i danych osobowych*, Warszawa 2009.

Cytuj jako:

Kozień A., *Uwarunkowania prawne zastosowania i rozwoju metaverse w medycynie*, „Ius Novum” 2025, nr 2(19), s. 141–154. DOI: 10.26399/iusnovum.v19.2.2025.18/a.kozien