KWARTALNIK NAUK O PRZEDSIĘBIORSTWIE

4/2023

prof. dr hab. Włodzimierz Szpringer
Szkoła Główna Handlowa
w Warszawie
Kolegium Nauk
o Przedsiębiorstwie
Katedra Prawa Administracyjnego
i Finansowego Przedsiębiorstw
e-mail: wszpri@sgh.waw.pl
ORCID: 0000-0003-3874-8906

Metaverse – nadmierny szum czy nowe szanse dla biznesu? (Cz. 2)

Metaverse – excessive hype or new business opportunities?

Słowa kluczowe:
metaverse, platformy cyfrowe, konkurencja, regulacja, ochrona danych oraz własności intelektualnej i przemysłowej, blockchain, NFT

Streszczenie: Celem artykułu (cz. 2) jest analiza metaverse z perspektywy kluczowych wyzwań dla regulacji. W dalszym ciągu analiza dotyczy kwestii, jakie to rodzi szanse i zagrożenia dla biznesu. Celem badań jest wskazanie kierunków rozwoju lub wykładni regulacji prawnych zwłaszcza dla zdecentralizowanych metaverse i ich wpływu na biznes (np. ochronę danych oraz własności intelektualnej i przemysłowej, blockchain i tokenizację NFT, kooperację i konkurencję), a także dla scentralizowanych metaverse (np. ochronę konkurencji i konsumenta). Metody badawcze – to przegląd literatury, prawa i orzecznictwa, z uwzględnieniem ekonomicznej analizy prawa.

Keywords:
metaverse, digital platforms, competition, regulation, protection of data and intellectual property, blockchain, NFT

Abstract: The aim of the article (part 2) is to analyze the metaverse from the perspective of key challenges for regulation. The analysis continues with the issue of opportunities and threats for business. The purpose of the research is to indicate the directions of development or interpretation of legal regulations, especially for decentralized metaverses and their impact on business (e.g. data protection and intellectual and industrial property, blockchain and NFT tokenization, cooperation and competition), as well as for centralized metaverses (e.g. competition and consumer protection). Research methods are – a review of literature, law and jurisprudence, including the economic analysis of law.

JEL:
K2, L5, G4, F6

Metaverse – potrzeba adaptacji mechanizmu ochrony danych

Tworzenie awatarów potrzebnych do „życia" i w metaverse oraz wykonywania różnych czynności wiąże się z udostępnianiem większej ilości danych korporacjom technologicznym. Platformy, które tworzą i zarządzają tym światem online, mogą wykorzystać te dane do usprawnienia i dostosowania swoich produktów i usług do indywidualnych oczekiwań użytkowników. Istnieją obawy, że wejście do metaverse może skutkować większą kontrolą działań osób fizycznych, które mogłyby być monitorowane i analizowane, zanim uzyskane dane zostaną sprzedane reklamodawcom. Naturalnie, w miarę jak przechwytuje się więcej danych osobowych do metaverse, wzrasta ryzyko kradzieży wrażliwych lub poufnych danych. Aby wykorzystać swój potencjał, jest wysoce prawdopodobne, że metaverse może potrzebować więcej czujników (sensorów) w domach i biurach. Cenne możliwości tych urządzeń w zakresie monitorowania zachowań i działań użytkowników w czasie rzeczywistym sprawią, że urządzenia te będą coraz bardziej podatne na ukierunkowane cyberataki. Metaverse – to koncepcja, która wykorzystuje środowisko cyfrowe do przenikania granic naszego fizycznego świata. Podobnie jak w przypadku platform mediów społecznościowych, kwestie prywatności będą na czele rozwoju metaverse, który zacznie zdobywać popularność wśród użytkowników. Jednym z aspektów metaverse, który budzi obawy dotyczące prywatności, jest ogromna ilość danych osobowych, które mogą być gromadzone od uczestniczących osób.

W porównaniu z tradycyjnymi mediami społecznościowymi platformy metaverse mogą śledzić osoby w znacznie bardziej intymny sposób. Firmy mogą w czasie rzeczywistym monitorować reakcje fizjologiczne i dane biometryczne, takie jak mimika twarzy, tonacje głosowe i parametry życiowe, podczas gdy uczestnicy znajdują się w metaverse. Ta głębia informacji pozwala firmom lepiej zrozumieć zachowania użytkowników, co z kolei może posłużyć do dostosowania kampanii reklamowych w wyjątkowo ukierunkowany sposób. Ponadto konsekwencje prawne korzystania ze sztucznej inteligencji („AI") będą kolejnym aspektem do rozważenia, biorąc pod uwagę jej powszechność w technologiach biometrycznych [Ahmad, Corovic, 2022].

W USA organizacja pozarządowa Truth in Advertising złożyła skargę do Federalnej Komisji Handlu (FTC) w związku z domniemanymi oszukańczymi praktykami reklamowymi popularnej platformy gier Roblox. Platforma jest nadal używana głównie w „dwóch wymiarach", ale kwestie poruszone w skardze pokazują, z jakimi wyzwaniami prawa reklamowego muszą mierzyć się użytkownicy metaverse. W skardze zarzuca się Robloxowi, że nie dokonuje wyraźnego rozróżnienia między treściami rozrywkowymi a treściami reklamowymi, uchwytnego dla rozsądnych konsumentów, a zwłaszcza dzieci. Platforma umożliwia użytkownikom tworzenie „advergames" łączących reklamy z grami. W skardze twierdzi się jednak, że rozróżnienie między grami (sponsorowanymi) tworzonymi przez reklamodawców a grami tworzonymi przez indywidualnych

użytkowników (bez treści promocyjnych) jest prawie niemożliwe, a sponsorowany charakter wydarzeń wirtualnych nie zawsze jest jasny. Te obawy wydają się uzasadnione, a zapobieganie im jest również kluczowe w metaverse. Wymagana jest dalsza kontrola prawna, gdy influencerzy wspierani przez reklamodawców pojawiają się jako awatary. Jeśli awatar nie jest kontrolowany przez influencera spoza metaverse, ważne jest, aby odnotować, jak daleko sięga odpowiedzialność influencera i gdzie zaczyna się odpowiedzialność reklamodawcy kontrolującego awatara.

W swojej obecnej formie internet opiera się na gromadzeniu danych, które niektórzy krytycy porównują do masowej inwigilacji. Firmy technologiczne i badacze zaczynają się zastanawiać, czy metaverse będzie czymś innym. W realistycznych światach nowe technologie będą pobierać dane na coraz bardziej szczegółowym poziomie – chód osoby, ruchy oczu, puls, emocje i nie tylko – znacznie bardziej poddając w wątpliwość istniejące zabezpieczenia [Uberti, 2022]. Metaverse chce zbierać nowe, niezbadane dane osobowe, nawet do punktu, w którym zauważa się i analizuje, gdzie oczy użytkownika kierują się na ekranie i jak długo patrzy na określone produkty [Preimesberger, 2022].

Zestawy słuchawkowe rzeczywistości wirtualnej (VR) mogą gromadzić więcej danych o nas niż tradycyjne ekrany, co daje firmom więcej możliwości gromadzenia i udostępniania tych danych w celu profilowania i reklamy. Mogą również dać pracodawcom więcej możliwości monitorowania naszego zachowania, a nawet naszych umysłów. Niewiele powstrzymuje rząd przed zdobyciem danych dotyczących ciała z technologii VR, i niewiele jest w stanie chronić nas i nasze dzieci od nieograniczonego gromadzenia danych i manipulacji psychologicznych. Grupa zajmująca się prawami cyfrowymi Electronic Frontier Foundation i Extended Reality Safety Initiative, organizacja non-profit opracowująca standardy i doradzająca prawodawcom w zakresie bezpieczeństwa w VR, podniosły alarm w związku z zagrożeniami dla prywatności, jakie stwarzają big-techy ze swoją wizją scentralizowanych metaverse – nie tylko dla pracowników, ale dla ludzi w ich życiu prywatnym [Hunter, 2022].

Badacze metaverse powinni bardziej zająć się kwestiami bezpieczeństwa, aby osiągnąć adekwatny poziom w stale rozszerzającej się przestrzeni metaverse. To nie technologia jest niebezpieczna, ale fakt, że potężne korporacje będą w stanie pośredniczyć we wszystkich aspektach naszego życia, sprzedając dostęp do naszych codziennych doświadczeń temu, kto zapłaci najwięcej. Wiem, że brzmi to jak dotyczące dzisiejszych mediów społecznościowych, ale w metaverse wtargnięcie w prywatność będzie o wiele bardziej głębokie. Aby to dokładnie opisać, uważam za pomocne wyróżnienie „trzech M" w metaverse, ponieważ podstawowe problemy sprowadzają się do jego zdolności do monitorowania nas, manipulowania nami i monetyzowania informacji o nas [Rosenberg, 2022].

Przejście z modeli opartych na reklamach na modele oparte na subskrypcji może być potężną poprawką, eliminującą motywację dostawców platform do monitorowania i manipulowania swoimi użytkownikami. Niestety działa to tylko wtedy, gdy

konsumenci są gotowi zapłacić za dostęp. Niektórzy będą skłonni zapłacić za bezpieczniejszy metaverse, który zainspiruje przedsiębiorców do tworzenia platform opartych na subskrypcji, ale nie możemy zakładać, że stanie się to normą. Obiecującym podejściem jest tworzenie zdecentralizowanych platform, które są kontrolowane przez użytkowników, a nie dostawców korporacyjnych. Nie jest to nowy pomysł, ponieważ światy VR o otwartym kodzie źródłowym sięgają dziesięcioleci, ale po dodaniu kryptowalut i inteligentnych kontraktów ten kierunek jest teraz bardziej obiecujący. Jednym z przykładów jest Decentraland.

Należy ograniczyć dozwolony poziom monitorowania. W metaverse dostawcy platform będą mieli dostęp do wszystkiego, co robimy, mówimy, dotykamy i widzimy – nie powinni mieć możliwości przechowywania tych danych przez okres dłuższy niż krótki czas wymagany do pośredniczenia w generowanych symulowanych doświadczeniach. To znacznie zmniejszyłoby stopień, w jakim mogą z czasem profilować nasze zachowania. Ponadto powinni być zobowiązani do informowania opinii publicznej o tym, co jest śledzone i jak długo jest ono przechowywane. Na przykład, jeśli monitorują wzrok klienta, musi on być wprost powiadomiony, kiedy takie śledzenie jest aktywne i jak jest używane.

Powinny istnieć ścisłe ograniczenia dotyczące dozwolonych rodzajów śledzenia i celów. Na przykład opinia publiczna powinna żądać ograniczeń dotyczących algorytmów reklamowych, które monitorują mimikę, modulacje głosu, postawę i parametry życiowe (w tym tętno, częstość oddechów, rozszerzenie źrenic, a nawet reakcję galwaniczną skóry). Ten rodzaj śledzenia brzmi ekstremalnie, ale jest to kierunek, w którym zmierzamy i nie jest to bardzo odległe. Jeśli nie będziemy ściśle regulować metaverse, te bardzo osobiste reakcje fizjologiczne będą wykorzystywane do dostrajania komunikatów marketingowych, dostosowując swoją strategię tak, aby wpływać na nas w czasie rzeczywistym. Ponadto musimy założyć, że metaverse odejdzie od tradycyjnych metod marketingowych, takich jak wyskakujące reklamy i filmy promocyjne, zamiast tego celując w nas w znacznie bardziej naturalny sposób, wprowadzając do naszego świata przedmioty i działania promocyjne, które wyglądają i są prawdziwe. Jeśli osoba trzecia płaci za wirtualne lokowanie produktu w rozszerzonym otoczeniu danego użytkownika, powinna być zobowiązana do poinformowania, że jest to celowe lokowanie, a nie przypadkowa interakcja, na którą właśnie się natknął klient.

To samo dotyczy sytuacji, gdy reklamodawcy kierują do nas symulowane persony, które angażują nas w coś, co wydaje się naturalne. Powinni być zobowiązani do jasnego i jawnego informowania nas o każdym kontakcie z agentami konwersacyjnymi kontrolowanymi przez inteligentne algorytmy, zwłaszcza gdy algorytmy mają ukryty program promocyjny. Staje się to jeszcze ważniejsze, gdy te algorytmy również monitorują nasze reakcje, na przykład oceniają naszą postawę i oddech, aby umiejętnie dostosować swoje podejście w czasie rzeczywistym. Ten rodzaj „interaktywnej manipulacji", zoptymalizo-

wany przez sztuczną inteligencję, nastąpi wkrótce i będzie w istocie przymusowy, o ile nie będzie ściśle regulowany.

Można rozważać trzy potencjalne modele zarządzania metaverse, dla których mamy analogie w świecie online: Walled Garden, Open House, formy hybrydowe. Opcja hybrydowa umożliwia twórcom ustalanie własnych zasad zarządzania, jednak kluczowe standardy prywatności danych, społeczności i bezpieczeństwa są regulowane przez państwo. Głównym standardem wśród nich byłoby wymaganie od firm hostujących metaverse, aby umożliwiały przenoszenie danych i interoperacyjność między innymi metaverse, aby zapewnić, że konsumenci nie są „zablokowani" do jednego dostawcy. Zmusza to dostawców do konkurowania jakością i usługami, zamiast polegać tylko na zawyżaniu kosztów zmiany, aby utrzymać użytkowników w swoich sieciach. Spośród tych modeli opcja hybrydowa może być najlepszym podejściem w świecie, w którym naszym celem jest zminimalizowanie ryzyka praktyk dyskryminacyjnych wynikających z nadużycia prywatności danych.

Tokenizacja, NFT a ochrona praw wyłącznych

W zdecentralizowanym metaverse handel wirtualnymi towarami i usługami, a także nazwami, ubraniami, akcesoriami noszonymi przez awatary, prowadzi do kilku problemów związanych ze znakami towarowymi i prawami autorskimi. Handel w metaverse wymaga tokenizacji i wirtualizacji produktów i usług istniejących w świecie rzeczywistym, co czyni tokeny NFT niezbędnym elementem metaverse. W metaverse istnieją różne formy własności intelektualnej, których jednym z aspektów są znaki towarowe, takie jak nazwa, logo, slogan, melodia (dźwiękowy znak towarowy), formy wizualne wszelkich znaków wyróżniających w metaverse, graficzny wygląd dóbr wirtualnych, które mogą być zakupione, nazwy awatarów i unikalne kolory (kolorowe znaki towarowe) mogą być prawnie chronione, co jest warte priorytetu podczas tworzenia IP wewnątrz metaverse, aby chronić markę.

Drugą stroną relacji między metaverse a znakami towarowymi jest to, że towary mogą być tokenizowane i potencjalnie kupowane w metaverse, w tym marki używane w metaverse. Właściciele marek, które nie obejmowały jeszcze towarów wirtualnych, usług wirtualnych, oprogramowania, grafiki itp. związanych z metaverse w klasach towarów i usług objętych ich znakami towarowymi będą zmuszeni do rewizji klas towarów i usług objętych ich znakami towarowymi i potencjalnie składać wnioski o nowe znaki towarowe w celu ochrony swojej marki i znaków towarowych, tak jak to już czyni wiele firm (np. znaki towarowe plików McDonald's dla wirtualnych restauracji w metaverse czy znaki związane z NFT i blockchain Victoria`s Secret).

Ochrona praw autorskich oprogramowania oraz dzieł graficznych i muzycznych, które stanowią część metaverse, jest oczywista i identyczna z tradycyjnym światem praw autorskich. Nie porusza żadnych szczególnych problemów w istniejącym środowisku praw autorskich. Nie dotyczy to jednak dzieł tokenizowanych, takich jak NFT dla cyfrowych i wirtualnych dzieł sztuki, które można nabyć w metaverse, gdzie ważne jest, aby nabywając NFT, posiadacz NFT nie nabywał żadnych praw autorskich do stokenizowanych utworów, na których opiera się NFT, i aby nie był uprawniony do korzystania z tego utworu w jakikolwiek inny sposób niż swobodne wykorzystanie w ramach dozwolonego użytku, które istniało do tej pory w prawie autorskim, bez zgody posiadaczy praw autorskich i bez płacenia tantiem. Ciekawe pytanie pojawia się, jeśli ktoś tokenizuje dzieło cyfrowe, którego nie stworzył: w tym przypadku naruszenie praw autorskich niekoniecznie zostanie stwierdzone w kontekście tokenizacji, ale wyświetlenie utworu online jako tokena w metaverse, nawet w formie miniatury, może stanowić naruszenie praw autorskich.

Niewymienne tokeny – zapisy własności cyfrowej przechowywane w łańcuchu bloków – będą podstawą gospodarki metaverse, umożliwiając uwierzytelnianie mienia, własności, a nawet tożsamości. Ponieważ każdy NFT jest zabezpieczony kluczem kryptograficznym, którego nie można usunąć, skopiować ani zniszczyć, umożliwia solidną, zdecentralizowaną weryfikację – czyjejś wirtualnej tożsamości i zasobów cyfrowych – niezbędną, aby społeczność metaverse mogła odnieść sukces i współdziałać z innymi społecznościami metaverse. Oprócz szumu o wielomilionowej sprzedaży dzieł sztuki cyfrowej, znaczenie NFT może leżeć w umożliwieniu rozkwitu czegoś, co przypomina prawdziwe społeczeństwo, oparte na wolnym rynku (w odniesieniu do towarów, usług i pomysłów), niezależnej własności i umowach społecznych w metaverse. Propozycja wartości firmy Decentraland dla twórców aplikacji polega na tym, że mogą oni w pełni wykorzystać ekonomiczne interakcje między swoimi aplikacjami a użytkownikami [FT, 2022].

Prawnicy eksponują wątpliwości prawne związane z transakcjami NFT. Takie obawy obejmują kwestie praw autorskich do NFT, relację między NFT a tokenizowanym dziełem. W 2021 r. dom aukcyjny Christie's sprzedał cyfrowy kolaż NFT amerykańskiego artysty Beeple'a, zyskując popularność i prowadząc do znacznej eksplozji na rynku NFT. Powszechne zastosowanie standardu ERC-721 opracowanego dla blockchain Ethereum zbiegło się z projektami NFT, które przyniosły NFT rozgłos. W 2017 r. firma Larva Labs była pionierem dużego eksperymentu ekonomicznego o nazwie CryptoPunks, który położył podwaliny pod współczesny ruch CryptoArt. Po sukcesie CryptoPunks, pierwsza wirtualna gra oparta na standardzie ERC-721, CryptoKitties, zyskała na znaczeniu, umożliwiając graczom handel, kolekcjonowanie unikatowych cyfrowych kreskówkowych wersji kotów w formie NFT [Xiao, 2022].

Właściciel marki Hermès podjął kroki prawne w USA wobec artysty Masona Rothschilda, twórcy NFT „MetaBirkin" zarzucając mu, że jego cyfrowa wersja słynnych torebek Birkin w formie NFT narusza prawa domu mody Hermès. W swojej skardze Hermès twierdzi, że „MetaBirkin" narusza znak towarowy „Birkin" i prawdopodobnie powoduje konfuzję wśród konsumentów, którzy mogą uznać, że artystyczne dzieła Rothschilda były autoryzowane, sponsorowane lub zatwierdzone przez Hermès. Rothschild argumentuje, że NFT stanowią jedynie artystyczną modyfikację słynnej torebki domu mody Hermès, co w jego ocenie nie wprowadza odbiorców w błąd w kwestii pochodzenia towarów oznaczonych spornym znakiem. Sąd oddala wniosek Rothschilda o oddalenie roszczenia potwierdzając jednocześnie, że również NFT może naruszać prawo ochronne do znaków towarowych. Sąd argumentuje, że NFT to po prostu kod wskazujący, gdzie znajduje się obraz cyfrowy i jego uwierzytelnianie, a użycie NFT do takiego uwierzytelnienia oraz umożliwienia późniejszej odsprzedaży i transferu nie czyni go towarem pozbawionym ochrony prawnej. To, że takie sprawy będą się coraz częściej zdarzały, pokazał przypadek sporu rozpoczętego przez klub piłkarski Juventus [Szambelan, 2023].

Również w tym kontekście bardzo istotne jest potwierdzenie amerykańskiego sądu, że użycie NFT do uwierzytelnienia obrazu i umożliwienia późniejszej odsprzedaży i transferu, nie uczyniło go towarem bez ochrony prawnej. Istotne jest odpowiednie zabezpieczenie praw tych podmiotów, które chcą być obecne w metaverse. Liczba sporów będzie rosła proporcjonalnie do liczby użytkowników nowej platformy. Brak odpowiedniej aktualizacji zgłoszeń znaków wraz z dostosowaniem wykazu towarów i usług do działania w metaverse może skutkować poważnym ograniczeniem lub utrudnieniami w ich skutecznej ochronie. Jednak największym wyzwaniem dla właścicieli znaków towarowych i praw autorskich będzie wykrywanie i egzekwowanie naruszeń w metaverse, dla którego zastosowanie sztucznej inteligencji jest niezbędne. Bez niej wykrywanie naruszeń napotykałoby na poważne przeszkody. Jeśli chodzi o egzekwowanie, transnarodowy i transgraniczny charakter metaverse wywoła pytania dotyczące obowiązującego prawa, jurysdykcji i właściwych organów, zwłaszcza jeśli działanie nie jest skierowane przeciwko dostawcy metaverse, ale przeciwko użytkownikowi metaverse ukrywającemu się za awatarem.

NFT to rozwiązanie oparte na technologii blockchain, która służy przede wszystkim do tokenizacji aktywów cyfrowych i handlu tymi tokenami. NFT mogą być czynnikami umożliwiającymi interoperacyjność między obszarami metaverse i umożliwiły i ułatwiły skierowanie handlu wirtualnymi aktywami w metaverse do gospodarki realnej. Emisja NFT wiąże się z kilkoma kwestiami prawnymi, ale w większości krajów nie jest jeszcze przedmiotem szczególnych regulacji. Poza aspektami związanymi z prawami autorskimi i znakami towarowymi, przy emisji NFT mogą pojawić się również ogólne kwestie umowne, cywilnoprawne, związane z inteligentnymi kontraktami, które są automatycznie

tworzone i realizowane na blockchain do sprzedaży NFT wraz z płatnością. W przypadku tych inteligentnych kontraktów zawsze istotnymi kwestiami są wykonalność i sprawdzalność, zwłaszcza w odniesieniu do kwestii anonimowości, ukrywania się za awatarami, ważności formalnej i postępowania w przypadku naruszenia umowy.

Pojawiają się również podstawowe pytania prawne dotyczące tego, które prawo krajowe ma zastosowanie do zakupu NFT w transgranicznych transakcjach metaverse oraz jakie prawa ma osoba nabywająca NFT. Jako analogię można użyć reżimu własności. W najbliższej przyszłości nadchodzące rozporządzenie MICA (projekt rozporządzenia w sprawie rynków kryptowalut) ureguluje sytuację prawną kryptowalut na poziomie UE, ale nie obejmie wszystkich kryptowalut, ponieważ obecny tekst Rozporządzenie MICA określiło jako wyjątek od zakresu rozporządzenia aktywa kryptograficzne, które są unikalne, ale nie można ich wymieniać z innymi aktywami kryptograficznymi, które mogą obejmować transakcje niefinansowe.

Nawet podstawowe zasady prawa cywilnego komplikują się w odniesieniu do metaverse i zawartych w nim awatarów. Na przykład, jeśli osoba, która stworzyła awatar umrze, to czy jej awatar, przypisane do niej (nabyte przez nią) zasoby wirtualne (NFT) mogą zostać przekazane? Z drugiej strony, czy sam awatar może „umrzeć" w metaverse – bez śmierci osoby, która go stworzyła? Czy dobra osobiste osoby, która utworzyła awatara, mają wpływ na naruszenie dobrej reputacji awatara w metaverse lub w przypadku zhakowania awatara i uzyskania dostępu do prywatnej komunikacji za pośrednictwem awatara (naruszenie prywatności) lub ich danych osobowych dotyczące awatara są niewłaściwie wykorzystywane, które dane osobowe dotyczą wirtualnego awatara i nie są tożsame z danymi osobowymi osoby, która stworzyła awatar (ochrona danych osobowych, prawo do informacyjnego samostanowienia)? Czy ktoś może zostać pozwany za naruszenia w metaverse przeciwko innemu awatarowi? A jeśli tak, to kto? Jakie prawa mają użytkownicy, którzy kupują wirtualne działki/grunty/nieruchomość w metaverse w tych obszarach? Czy inni użytkownicy mogą bez pozwolenia wejść do takich obszarów w metaverse ze swoim awatarem? Jest tak wiele kwestii, dla których nie ma ustawodawstwa ani orzecznictwa, a tylko niektóre z nich można rozwiązać w ogólnych warunkach korzystania z metaverse, które są publikowane przez samych dostawców metaverse.

Przełomowe orzeczenie Sądu Najwyższego Wielkiej Brytanii w sprawie Lavinia Deborah Osbourne przeciwko Ozone Networks Inc. potwierdziło, że NFT są uważane za własność. Sprawa Osbourne z pewnością stanowi kamień milowy w traktowaniu NFT przez sądy brytyjskie. Wygląda na to, że sądy zmierzają w tym kierunku, próbując chronić zasoby cyfrowe. W 2022 r. Sąd Najwyższy w Singapurze jako pierwszy w Azji wydał potwierdzenie własności w celu zamrożenia NFT na blockchainie Ethereum w imieniu singapurskiego inwestora przeciwko nieznanemu pozwanemu na platformie cyfrowej [Whittaker, 2022].

Powstanie nowej klasy aktywów wirtualnych, rosnący popyt i wartość, a także brak regulacji oznaczają, że istnieje poważne ryzyko i wyzwania stojące przed firmami zaangażowanymi w metaverse. Zarządzanie tymi zagrożeniami raczej wcześniej niż później powinno być jednym z najważniejszych priorytetów każdej firmy cyfrowej. Przyjęcie podejścia opartego na ryzyku, które zapobiega niechcianym transakcjom, minimalizuje ryzyko i zmniejsza ryzyko nielegalnej działalności dzięki najlepszym praktykom i zaawansowanemu oprogramowaniu, będzie kluczem do przygotowania się na bardziej rygorystyczne środowisko regulacyjne, które z pewnością nastąpi. Podczas gdy klasa aktywów NFT kwitnie, jej wzrost mógł wyprzedzić globalne ramy prawne. Jest wysoce prawdopodobne, że – jako bardzo wartościowy, transgraniczny i w pełni cyfrowy zasób – NFT nadal będą celem cyberprzestępców. Przejęcia kont, kluczowe luki w zabezpieczeniach i próby phishingu już nękają branżę. Anonimowość świata blockchain i scentralizowane rynki NFT sprawiają, że NFT są szczególnie atrakcyjne dla przestępców. Brak weryfikacji tożsamości oznacza, że oszuści mogą twierdzić, że posiadają token i sprzedać go ze szkodą dla twórcy i rynku.

Wiele platform metaverse zastrzega sobie prawo do zmiany swoich warunków świadczenia usług w dowolnym momencie, nawet bez powiadomienia. Oznacza to, że użytkownicy powinni stale aktualizować i ponownie czytać swoje warunki korzystania z usługi, aby upewnić się, że ich „zakupione" zasoby i całe konto nie są zaangażowane w ostatnio zabronione działania, które mogą grozić usunięciem konta. Sama technologia nie może utorować drogi do faktycznej własności zasobów cyfrowych w metaverse. NFT nie mogą obejść scentralizowanej kontroli, którą platforma metaverse obecnie posiada i nadal będzie sprawować na podstawie umownych warunków użytkowania. Dominantą jest zatem prawo umów, a nie prawo własności. Wielu uważa, że niezamienne tokeny stanowią niezaprzeczalny dowód własności. Jednak obecnie wirtualna własność gruntu podlega prawu umów, a nie prawu własności [Das, 2022].

Oznacza to, że platformy metaverse mogą usuwać lub rozdawać wirtualne dobra użytkowników poprzez odłączenie treści od swoich kodów identyfikacyjnych NFT, a wszystko to w granicach prawa. Zasadniczo zakup NFT nie daje użytkownikom prawa własności do zasobu cyfrowego. Zakup oznacza raczej, że platforma umożliwi użytkownikowi dostęp do wspomnianego zasobu cyfrowego przez nieokreślony czas. Wiele metaverse i platform NFT ma prawo blokować dostęp do zasobu cyfrowego zgodnie z ich warunkami użytkowania. Dodatkowo, jeśli Sandbox uzna, że użytkownik ingerował w możliwość korzystania z platformy przez innego użytkownika, zastrzega sobie prawo do zawieszenia lub nawet usunięcia konta użytkownika. Ponadto platforma zastrzega sobie prawo do usunięcia samego użytkownika.

Rodząca się natura metaverse pozostawia pewne prawa własności intelektualnej w dużej mierze nierozstrzygnięte. Technologie metaverse mają szeroki zakres, wywołując unikatowy zestaw problemów patentowych dla firm, które chcą chronić swoje IPR

w metaverse. W przypadku obejmujących technologię zestawów słuchawkowych, kontrolerów, oprogramowania, interfejsów użytkownika, serwerów sieciowych, mocy, procesorów, przepustowości i opóźnień sieci, sztucznej inteligencji i uczenia maszynowego oraz transakcji blockchain ważne jest, aby myśleć całościowo o technologii i wynalazkach w metaverse. Ponieważ inne firmy w tej dziedzinie aktywnie dążą do uzyskania podobnych patentów w coraz szybszym tempie, wielu wczesnych użytkowników, głównie bigtechy, chce uzyskać korzyści.

Metaverse – wyzwania dla ochrony konkurencji

Wirtualne światy (np. Second Life) pozwoliły firmom na ekstrakcję wartości, czyli możliwość stworzenia wirtualnej wartości, która musi zostać przełożona na rzeczywistą. Jednak eksperymenty firm ujawniły kilka poważnych problemów, z którymi trzeba się uporać. Główny problem polega na tym, że kontakt z awatarami nie oznacza automatycznie dotarcia do potencjalnych klientów. Potrzeby, wartości i preferencje awatarów zależą od cech metaverse, a nie od zachowań ludzi w świecie rzeczywistym. Dlatego, gdy firmy zamierzają ustanowić skuteczny proces ekstrakcji wartości, muszą ocenić potencjalną niezgodność między kontekstem wirtualnym a rzeczywistym. Oznacza to zbadanie wpływu ekstrakcji wartości na inne procesy związane z łańcuchem wartości [Rosita Cagnina, Poian, 2008]. Powstaje pytanie, w jaki sposób firmy, osoby prywatne i celebryci mogą wykorzystać metaverse jako rozszerzenie marki, poszerzanie swojego zasięgu i łączenia się z innymi w wirtualnym świecie [Bushell, 2022].

Charakter konkurencji w metaverse będzie prawdopodobnie zależał od struktury platformy metaverse i ich aplikacji oraz ich mechanizmu współdziałania. Na tym etapie otwartość, mobilność i łączność użytkowników, produktów i usług w metaverse są często przedstawiane jako podstawowe cechy metaverse i jego konkurencyjnego środowiska. Ale co to będzie oznaczać w praktyce, dopiero się okaże. Jeśli jedna lub więcej platform metaverse zasadniczo stanie się zamkniętym ekosystemem, konsumenci nie będą mogli swobodnie podróżować między różnymi „światami" metaverse. Nie byliby na przykład w stanie przenosić wirtualnych towarów lub usług z jednej platformy metaverse na drugą. Mogłoby to – z konsumentami w zamkniętym systemie – doprowadzić do pojawienia się strażników, którzy kontrolują dostęp do metaverse i jego użytkowników, podobnie jak zmiany zaobserwowane w wielu podstawowych usługach platform określonych w niedawno uzgodnionej regulacji DMA. Co więcej, rynki metaverse mogą czerpać korzyści z silnych efektów sieciowych i być podatne na „przechylanie", ponieważ firmy i użytkownicy zwykle czerpią korzyści z posiadania masy krytycznej innych użytkowników obecnych na tej samej platformie. Kiedy tak się dzieje, nowym konkurentom bardzo trudno jest wejść na rynek,

a istniejącym konkurentom pozostaje dalsza ekspansja [Schickler, 2022; Mackenzie, Westrup, Mantine, 2022].

W takim scenariuszu zachowanie firmy, która zasadniczo kontroluje dostęp do „swojego" metaverse, może na wiele sposobów ograniczać jej konsumentów, partnerów biznesowych i konkurentów. Strażnik metaverse może na przykład nakłonić użytkowników do przyjęcia określonych usług lub produktów, łącząc je z „niezbędnym" sprzętem lub oprogramowaniem metaverse. Mogą narzucić wygórowane ceny za dostęp do metaverse lub niektórych swoich ofert opartych na metaverse. Mogą zawierać umowy na wyłączność z niektórymi zewnętrznymi dostawcami usług metaverse, zmniejszając wybór dla konsumentów i ograniczając dostęp konkurentów do ich platformy. Mogliby również wykorzystać swój unikatowy wgląd w zachowania użytkowników (na podstawie dostępu do określonych danych), aby wzmocnić swoją siłę rynkową na rynku metaverse i poza nim.

Te potencjalne wyzwania związane z konkurencją nie są nowe – wiele z nich zaobserwowano już na innych rynkach i ekosystemach cyfrowych. Jednocześnie, ponieważ metaverse wciąż bardzo się kształtuje, istnieją również możliwości upewnienia się, że pewne problemy z innych kontekstów cyfrowych nie zostaną zaimportowane do metaverse. Zamiast tego można też wyobrazić sobie metaverse jako otwarte, konkurencyjne środowisko, zorganizowane na podstawie wielu interoperacyjnych światów, pomiędzy którymi użytkownicy mogą łatwo przenosić wirtualne towary i usługi w bezpieczny sposób. Oznaczałoby to na przykład, że awatary mogłyby bezproblemowo przemieszczać się z jednego do drugiego markowego środowiska. Jest jednak prawdopodobne, że wymagałoby to szeroko zakrojonej współpracy w zakresie podstawowych norm i technologii, co samo w sobie, w zależności od okoliczności, mogłoby mieć skutek ograniczający konkurencję.

Analiza potencjalnych problemów antymonopolowych związanych z metaverse będzie zależeć od rodzaju wirtualnej przestrzeni, która się pojawi. Czy będzie wiele oddzielnych przestrzeni wirtualnych, tak jak istnieje wiele witryn hostowanych przez różne podmioty? A może będzie istniał jeden nadrzędny metaverse, z którego inni będą musieli wynajmować swoje powierzchnie, oferując dostęp podobny do „centrum handlowego" do wszelkiego rodzaju ofert komercyjnych i niekomercyjnych? Czy dostęp do metaverse będzie niezależny od bramy dla użytkowników i strumieni finansowych, czy też niektóre przestrzenie w metaverse będą dostępne tylko za pośrednictwem określonych urządzeń (takich jak zestawy słuchawkowe VR niektórych marek)? Chociaż odpowiedzi na te pytania nie są pewne, prawo antymonopolowe z pewnością odegra pewną rolę w rozwoju metaverse. Dwa główne aspekty tego będą dotyczyć (1) interoperacyjności oraz (2) dominacji i monopolizacji. Pewne inspiracje są już obecnie dostępne w orzecznictwie w sprawach bigtechów (np. Amazon, Apple, Google, Facebook). Należy wszakże mieć na uwadze, aby regulacja nie blokowała innowacji [Megale, 2022].

Interoperacyjność leży u podstaw tego, jaki rodzaj metaverse się pojawi. Interoperacyjność opisuje, kiedy systemy mogą wymieniać informacje w sposób, który pozwala jednemu systemowi korzystać z funkcji innego systemu. Dzięki dobrze zdefiniowanym i otwartym standardom interoperacyjność obniżyłaby bariery wejścia na rynek dla konkurentów metaverse i umożliwiłaby programistom i innym użytkownikom czerpanie korzyści z efektów sieciowych. (Efekt sieci pojawia się, gdy użyteczność usługi dla użytkownika wzrasta wraz z dodawaniem większej liczby użytkowników do tej usługi.) Potencjalne funkcje metaverse, takie jak pierwotny i wtórny rynek dóbr wirtualnych, skorzystałyby na posiadaniu więcej użytkowników uczestniczących w tych rynkach. Wartość tych wirtualnych towarów wzrośnie, jeśli interoperacyjność połączy transakcje kupców i użytkowników między przestrzeniami różnych dostawców.

Decyzje dotyczące interoperacyjności budzą wszelako również obawy antymonopolowe. Mimo że większość zainteresowanych stron odnosi korzyści z interoperacyjności czy multihomingu, firmy muszą uważać, aby uniknąć naruszeń przepisów antymonopolowych, uzgadniając jakiekolwiek standardy z konkurencją i potencjalnie dzieląc się strategicznymi informacjami. Agencje antymonopolowe są często podejrzliwe w stosunku do takiego udostępniania informacji. Niedawna praktyka w Europie sugeruje nawet, że ustanawianie standardów antyinnowacyjnych przez garstkę dużych graczy może stanowić zachowanie kartelowe i prowadzić do grzywien w wysokości miliardów dolarów. Jednocześnie jednak zarówno organy regulacyjne, jak i prywatni powodowie w Stanach Zjednoczonych i Europie próbowali wymagać od dostawców, aby ich usługi były interoperacyjne [Rosehill, Crauthers, 2022; Gordon, 2022].

W ostatnich latach w kręgach antymonopolowych popularność zyskał termin „zabójcze przejęcie" oraz „drapieżna innowacja". „Zabójcze przejęcia" odnoszą się do przejęć przez duże firmy innowacyjnych, rodzących się konkurentów wyłącznie (lub przede wszystkim) w celu przerwania innowacyjnych projektów konkurentów i uprzedzenia przyszłej konkurencji. Ale w przypadku „zabójczego przejęcia" rodzący się konkurent zwiększyłby konkurencję, a tym samym zagroziłby zmniejszeniem udziału w rynku i rentowności większej firmy. FTC złożyła pozew przeciwko Meta, oskarżając firmę o nielegalne utrzymywanie monopolu na sieci społecznościowe. Skarga Komisji zawiera zarzuty, że Meta wykorzystała przejęcie Instagrama w 2012 r. i WhatsApp w 2014 r. do utrzymania swojej monopolistycznej pozycji. Istnieją teraz obawy, że Meta może stosować tę samą taktykę w metaverse. Oprócz przejęcia Oculus, Meta kupiła szereg innych firm powiązanych z metaverse. Meta firma ogłosiła, że przejmuje firmę Within, która tworzy produkty, treści, oprogramowanie i narzędzia dla wirtualnej i rozszerzonej rzeczywistości. FTC zablokowała także przejęcie przez Meta firmy Within Unlimited, która opracowuje aplikacje na urządzenia VR, konkurencyjne względem Meta. Takich przykładów ciągle przybywa [Petrosyan, 2022].

Wnioski

Biznes w zdecentralizowanych metaverse będzie opierał się głównie na DLT blockchain kryptowalutach i tokenach NFT, podnosząc kwestie interoperacyjności, własności, właściwego użytkowania praw własności intelektualnej i przemysłowej oraz możliwości przenoszenia praw. Niezbędne jest wyjaśnienie statusu własności intelektualnej i przemysłowej w metaverse, zwłaszcza NFT, gdyż obecnie nie jest jasne, czy działa w tej kwestii prawo własności, czy tylko prawo umów, jednostronnie interpretowane przez operatorów platform metaverse. Zagrożenia dla konkurencji są związane zwłaszcza z działalnością wielkich platform cyfrowych (bigtechów), które budują scentralizowane metaverse (np. Horizon Worlds) i opanowują produkcję sprzętu i oprogramowania. Stąd tak ważne znaczenie interoperacyjności, multihomingu i niedyskryminacji, kontroli karteli i fuzji w tym obszarze, zwłaszcza w zakresie tzw. drapieżnych innowacji i zabójczych przejęć. Ignorując szum informacyjny, można uznać, że metaverse powinien znajdować się na mapie drogowej innowacji większości firm, ponieważ może wpływać na wiele linii biznesowych, sektorów przemysłu i regionów geograficznych.

Bibliografia

Ahmad I., Corovic T. [2022], *Privacy in a Parallel Digital Universe: The Metaverse*, Data Protection Report, January 25, https://www.dataprotectionreport.com/2022/01/privacy-in-a-parallel-digital-universe-the-metaverse/ (data dostępu: 1.06.2023).

Bushell Ch. [2022], *The Impact of Metaverse on Branding and Marketing – A Study of How Individuals and Celebrities Use Metaverse as a Brand Extension, and the Implications for Marketing*, June 23, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144688 (data dostępu: 1.06.2023).

Das P. [2022], *Your Ownership of Metaverse land is not Legal under Property Law: Here's Why*, IndustryWired, April 29, https://industrywired.com/your-ownership-of-metaverse-land-is-not-legal-under-property-law-heres-why/ (data dostępu: 1.06.2023).

FT [2022], *Financial services and augmented reality*, Financial Times, July 4, https://www.ft.com/content/9fd75817-1ee1-4a44-8d77-bc26a5747aed (data dostępu: 1.06.2023).

Gordon M. [2022], *Meta hits back against U.S. regulators who say it's creating a VR monopoly*, Fortune, October 14, https://fortune.com/2022/10/14/meta-hits-back-against-us-regulators-creating-vr-monopoly-within-unlimited-supernatural/ (data dostępu: 1.06.2023).

Hunter T. [2022], *Surveillance will follow us into 'the metaverse,' and our bodies could be its new data source*, The Washington Post, January 13, https://www.washingtonpost.com/technology/2022/01/13/privacy-vr-metaverse/ (data dostępu: 1.06.2023).

Mackenzie R., Westrup M., Mantine M.A. [2022], *Managing antitrust & competition risk*, Reed Smith, 1 August, https://www.reedsmith.com/en/perspectives/metaverse/2022/08/managing-antitrust-and-competition-risk (data dostępu: 1.06.2023).

Megale L. [2022], *(Meta) verse as the next escaper form competition public enforcement*, „Market and Competition Law Review", vol. 6(2), s. 15–50, https://betteregulation.lumsa.it/metaverse-next-escaper-form-competition-public-enforcement-luca-megale (data dostępu: 1.06.2023).

Petrosyan G. [2022], *Antitrust Enforcers Enter the Metaverse*, Constantine Cannon, March 17, https://constantinecannon.com/antitrust-group/antitrust-today-blog/antitrust-enforcers-enter-the-metaverse/ (data dostępu: 1.06.2023).

Preimesberger Ch.J. [2022], *Metaverse vs. data privacy: A clash of the titans?* Venture Beat, January 28, https://venturebeat.com/2022/01/28/metaverse-vs-data-privacy-a-clash-of-the-titans/ (data dostępu: 1.06.2023).

Rosehill D., Crauthers R.S. [2022], *Antitrust: Into the Metaverse*, Wilson Sonsini, March 18, https://www.wsgr.com/en/insights/antitrust-into-the-metaverse.html (data dostępu: 1.06.2023).

Rosenberg L.B. [2022], *Regulating the Metaverse, a Blueprint for the Future*, Springer Link, August 26, https://link.springer.com/chapter/10.1007/978-3-031-15546-8_23 (data dostępu: 1.06.2023).

Rosita Cagnina M., Poian M. [2008], *How to Compete in the Metaverse: The Business Models in Second Life*, U of Udine Economics Working Paper No. 01–2007, Jan 31, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1088779 (data dostępu: 1.06.2023).

Xiao B. [2022], *Copyright law and non-fungible tokens: experience from China*, „International Journal of Law and Information Technology", vol. 30(4), https://academic.oup.com/ijlit/article/30/4/444/7076730? searchresult=1 (data dostępu: 1.06.2023).

Schickler J. [2022], *EU Antitrust Officials Are Worried About Competition in the Metaverse*, Coin Desk, October 19, https://www.coindesk.com/policy/2022/10/19/eu-antitrust-officials-are-worried-about-competition-in-the-metaverse/ (data dostępu: 1.06.2023).

Szambelan T. [2023], *Sprawa naruszenia praw do znaku luksusowej marki Hermès w Metaverse nabiera rozpędu*, Kochański&Partners, 9 stycznia, https://www.kochanski.pl/sprawa-naruszenia-praw-do-znaku-luksusowej-marki-hermes-w-metaverse-nabiera-rozpedu/ (data dostępu: 1.06.2023).

Uberti D. [2022], *Come the Metaverse, Can Privacy Exist?* https://www.wsj.com/articles/come-the-metaverse-can-privacy-exist-11641292206 (data dostępu: 1.06.2023).

Whittaker R. [2022], *A pivotal judgment on NFTs in the UK? Osbourne v (1) Persons Unknown and (2) Ozone Networks Inc.*, June 22, https://www.scl.org/articles/12631-a-pivotal-judgment-on-nfts-in-the-uk-osbourne-v-1-persons-unknown-and-2-ozone-networks-inc (data dostępu: 1.06.2023).