

Pirkad a metaverzumban: az új virtuális világ egyes adatvédelmi és társadalmi kérdéseiről



A metaverzum egy sok tekintetben futurisztikus és lenyűgöző virtuális világot kínál, amelyben a felhasználó újszerű módon lesz képes feloldódni a digitális környezetben. A tanulmány arra mutat rá, hogy az új technológia csak részben vet fel újszerű adatvédelmi problémákat. A magánszférát érintő kérdéseken túl néhány olyan területet is elemeztünk röviden, amelyek csupán illusztrációi a metaverzumot, valamint általában az internethasználatot érintő társadalmi kérdések sokaságának.

A metaverzum előképei már léteznek, a virtuális valóságban zajló játékok tapasztalatai sok min-dent előrevetítenek abból, ami a metaverzumot a jövőben jellemezni fogja. Az új virtuális közeg sem-miképpen sem lesz jogon kívüli terület, ott sok más követelmény mellett az adatvédelmi szabályozás is érvényesítendő lesz. A metaverzum a magánszférát sok szempontból érinteni fogja. Az avatárokhoz kapcsolódó adatokat személyes adatnak kell tekinteni, amelyek védelme érdekében intézkedéseket kell majd tenni. Különös jelentősége lesz a *privacy by design* elvnek a rendszer tervezése során.

Az adatkezelők várhatóan sok esetben osztozni fognak az adatkezelői felelősségen más adatke-zelőkkel, és a közös adatkezelői minőség minden bizonnyal számos üzleti modellben érvényesülni fog. Az adatalanyok önkéntelenül is sok személyes adatot fognak feltárni magukról a metaverzumban.

Ahhoz, hogy a metaverzumban a magánszféra megőrizhető legyen, a tervezés során védelmi funkciókat kell beépíteni. Ilyen a fizikai távolságot szimuláló funkció, de sok más intézkedést kell elérhetővé tenni, például a mások figyelme elől elvonulni képes megoldásokat. A klasszikus adat-biztonsági problémák a metaverzumban is jelen lesznek. A hozzáféréskontroll érzékeny kérdéseket vet fel, hiszen a biometrikus azonosítók adott esetben magasabb biztonságot képviselhetnek, míg a kezelésük önmagában is magas kockázatúnak tekintendő.

A metaverzum jogi és magánszféra-védelmi kérdései terén számos további kutatásra lesz szükség a társadalmi hatások pontos feltérképezéséhez.

Bevezetés

Az embert mindig is foglalkoztatta annak gondolata, hogy új világot teremtsen, egy világot a másik világban. Az álmok sokszor nehezen megfejtethető élményvilága gyakran jelentős hatást gyakorolt az ébredés utáni gondolatokra, döntésekre. Az em-beri gondolkodásban kitörölhetetlenül jelen van az a misztikumba hajló vágy, hogy az ember létrehozzon egy olyan közeget, ahol szabadabbnak érezheti magát, a való világban megtapasztalt korlátok elmosódhatnak, és a lehetőségek tárháza szinte meseszerű távlatokat nyit. A technológiával is játszó ember, az örök *homo ludens*

nem kétséges, hogy át kívánja lépni azt a küszöböt, amely a metaverzum irányába mutat. A sikerét előre nehéz megbecsülni, de annyi bizonyos: bele próbál kóstolni, és saját bőrén akarja meg tapasztalni a felhasználók sokasága a metaverzum világát.

Sok évvel ezelőtt egy külföldi utam során az ismeretlen utcákon sétálva fogalmazódott meg bennem a gondolat: milyen nagy segítség lenne egy olyan szolgáltatás, amely a hagyományos térképnél többet nyújtana, és az utcaképet a maga teljességében jelenítené meg, támogatva az ismeretlen helyen járó turistát. Akkor a street view szolgáltatás még nem volt elérhető, és fiatal adatvédelmi jogászként gyorsan el is hessegettem magamtól a gondolatot, hiszen egy ilyen adatfelvétel túlzott beavatkozást jelentene a helyi lakosság magánszférájába – gondoltam akkor. Azóta tudjuk, hogy a gondolat mások fejében is megfordult, és azóta világszerte elérhető és népszerű lett az online térképek utcakép funkciója.

Miért jut ez a metaverzum kapcsán eszembe? Azért, mert akkor, lassan két évtizede úgy éreztem, hogy a street view szolgáltatás az utcán, elszórt módon készített felvételekhez képest jelentős, minőségi lépést jelentene az adatvédelemhez fűződő jog zsugorításában, a magánszféra szűkítésében. A metaverzum kapcsán is felmerül a kérdés: az építőelemek már ismertek, tehát rendelkezésünkre áll a world wide web, vagyis az internet, a világ legutolsó zugairól készült képanyag szintén elérhető, a kiterjesztett és virtuális valóság eszközei szintén kézzelfoghatóak. Innen már csak néhány (igaz, bonyolult) lépés, és mindezek kombinációjából összegeyúrható az a világ, amelyet metaverzumnak nevezünk.

Van-e itt olyan változás, amely azt indokolná, hogy a metaverzumról úgy beszéljünk, mint ami egészen új minőséget hoz létre? Vagy az, ami újnak tűnik, talán nem is annyira idegen és újszerű ahhoz képest, mint amit már ismerünk és a hétköznapiakban meg tapasztaltunk?

Az európai adatvédelmi biztos elemzést végzett annak feltárására, hogy a következő években mely technológiák érdemlik a legnagyobb figyelmet adatvédelmi szempontból. A 2022/23-as jelentés öt technológiát említ: a központi bank digitális fizetőeszközét, az álhírfelismerő rendszert, a szintetikus adatokat, a federált/kollaboratív tanulást (*federated learning*) és a metaverzumot.¹ Témánk nem véletlenül keltette fel az információs társadalmi témákat kutató szakemberek érdeklődését.

Melyek a metaverzum adatvédelmi kérdései? Van-e ezekre helyes, megnyugtató válasz? Az írás kiindulópontjai ezek a kérdések, amelyekre válaszokat keresünk. Az írás közel sem átfogó elemzés, és a szerző nem is törekszik erre. A tanulmány megírásának célja, hogy további hazai kutatásokra és publikációkra sarkallja az olvasót, ha úgy tetszik, vitaindító szereppel született.

¹ Az európai adatvédelmi biztos Tech Sonar jelentése: European Data Protection Supervisor: *Tech Sonar 2022–23 report*. 10.

Mi a metaverzum?

A metaverzum elnevezés Neal Stephenson amerikai író science fiction regényéből származik. Az 1992-ben publikált *Snow Crash*² írja le azt a világot, amelyben az emberek a fizikai világgal párhuzamosan létező metaverzumban is élik az életüket VR (*virtual reality*) eszközök segítségével. A metaverzumban a személyek digitális avatárjukon keresztül jelennek meg, ilyen módon kettőződik meg az ember által tapasztalt világ a digitális világ segítségével.³

A metaverzum leírása természetesen filozófiai kérdések sorát veti fel, mi most itt ebben a tanulmányban mégis elsősorban az egyes ember oldaláról, az ő érdekei és jogai szempontjából közelítünk ehhez az új jelenséghez.

Egyetlen filozófiai jellegű kérdés mégis engedtessek meg a jogász szerzőtől. A számítógép az ember lehetőségeinek javítására hivatott, ezek a képességek, a számítási kapacitás lenyűgöző volta tette annak idején, a 20. században „új technológiává”. A hétköznapi ember számára a számítógép akkor vált életközelié, amikor megjelentek a személyi számítógépek, és a háztartásokban nemcsak a készülékek, hanem a szoftver is irodai asszisztens vagy népszerű digitális játékok formájában az élet részévé vált. A viselhető eszközök, valamint az IoT még egy jelentős lépést jelent az emberközelség útján, a való és a virtuális világ közelítésében.

Amire rá kívánok itt mutatni, az egy olyan tulajdonsága a metaverzumnak, amely a sajátosságainak lényegét adja: az ember már nemcsak a bináris számrendszerrel leírható eszközök használójaként, hanem önmaga is egy bináris „adattömegként” simul bele a környezetébe. A metaverzum annak az élményét kínálja, hogy egyszerre többen tapasztaljuk meg ugyanazt a virtuális világot, és abban egymáshoz is kapcsolódni tudunk, legyen szó játékról, kereskedelemről, virtuális utazásról vagy bármilyen közös tevékenységről.

Jaron Lanier aggodalma juthat itt eszünkbe, aki szerint az utóbbi évtizedekben a technológia mintha lefokozta volna a személyközi interakciókat, pedig itt a legfontosabb kérdés, hogy a technológia hogyan változtatja meg az embert.⁴ Hogyan lehet tehát a metaverzumban úgy mozogni, úgy „létezni”, hogy mindeközben ne csak jogainkat, hanem *emberségünk* lényegét is megőrizzük? Alan F. Westin szintén, és meglehetősen korán, már az 1960-as években felhívta a figyelmet a technológiával együtt járó elembertelenedésre.⁵

² Az összefoglaló forrása: Snow Crash Summary and Study Guide. *SuperSummary*.

³ A szerzővel készült egyik interjúban úgy vélekedett, hogy a metaverzum *Snow Crash*-ben leírt gondolatát azért is használják fel az új technológia sorvezetőjeként, mert a fejlesztőknek egyszerűbb egy kész koncepcióra építeni, mint egy új elgondolás kidolgozásán hosszasan fáradozni. Úgy fogalmaz: a science fiction író a technológiai iparra legnagyobb hatást gyakorló pozíció. Az interjú elérhető online: Neal Stephenson on the Future of the Metaverse. *YouTube*.

⁴ Jaron Lanier: *You Are Not a Gadget*. London, Penguin Books, 2011. 4.

⁵ Alan F. Westin (szerk.): *Information Technology in a Democracy*. Cambridge, MA, Harvard University Press, 1971.

Próteusz-szindrómaként⁶ említi a tudomány azt a jelenséget, amikor a videójátékban részt vevő személy az avatárjával akarva-akaratlanul azonosul, és a játékban felvett szerepének hatása a való világban is érvényesül.⁷ A játékon belül is megfigyelhető az avatár hatása a viselkedésre, így például normál testsúlyú avatárral rendelkező játékosok nagyobb eséllyel fognak sportolni, vagy a magasabb avatárok mögötti játékosok nagyobb önbizalommal rendelkeznek, mint a náluk kisebb társaik. De nem csupán a virtuális közegben való viselkedésre hathatnak ki az avatár jellemzői, hanem az offline életben is képes alakítani a személyiséget.

Azok a játékosok, akik részt vettek a „Papers, Please” nevű, disztópikus körülmények között játszódó bevándorlási hivatali szimulációs játékban, azok később a bevándorló háttérű személyekkel kevésbé segítőkész módon bántak.⁸ Pozitív példa is hozható ugyanakkor, így például a szuperhőst játszó felhasználók mintha az offline világba visszalépve segítőkészebbé váltak volna. De akár terápiás távlatokat is nyit az avatárokkal való összefonódás, gondolni lehet itt fóbák kezelésére vagy személyes képességek, lehetőségek javítására.⁹

Úgy tűnik tehát, hogy az emberi méltóság védelmének kérdései a technológia használata kapcsán különös élességgel vetődnek fel: nem önmagában az új technológia, hanem annak használata, nem megfelelő alkalmazása vagy éppen az ismeretek hiánya, a védekezési mechanizmusok kiiktatása vet fel fontos kérdéseket.

Az alábbi jogi elemzésben az érintetti jogokról, adatvédelmi alapelvekről és ezek európai, illetve globális összefüggéseiről lesz szó. Mindezek háttérben azonban ott állnak a most megfogalmazott kérdések, amelyek foglalkoztatják a szerzőt, és valószínűleg a kedves olvasót is.

A metaverzum technológiai oldala

2023-ban a metaverzum még csak egyes elemeiben rajzolódik ki. Nem egy már jelenleg is létező, hanem jövőbeni technológiáról beszélünk, de ahhoz már elég információ áll rendelkezésre, hogy a körvonalait felmérhessük: miként fog felépülni, milyen funkciókat fog kínálni. Online és offline közösségek összekapcsolódását kell elképzelnünk, ahol a felhasználók akár szakmai, akár személyes megfontolások alapján építhetnek ki közösségeket, szórakozhatnak, kereskedhetnek virtuális

⁶ Próteusz görög tengeristenség, aki a mitológia szerint jóstehetséggel rendelkezett, de mivel százféle alakot tudott öltetni, mindig kicsúszott azok kezéből, akik jóslásra akarták kényszeríteni. Online forrás: Próteusz. *Arcanum*. Érdekes megfigyelni, hogy a legújabb technológia jellemzőinek leírásakor is antik gyökerekhez nyúl vissza a tudomány.

⁷ Kim Szolin et al.: “I Am the Character, the Character Is Me”: A Thematic Analysis of the User-Avatar Relationship in Videogames. *Computers in Human Behaviour*, 143. (2023), 3.

⁸ Szolin et al. (2023): i. m. 3.

⁹ Proteus effect. *Tech Target*.

és valóságos javakkal, szolgáltatásokkal.¹⁰ Nagy technológiai vállalatok, mint a Facebook (Meta), a Microsoft, a Tencent vagy az NVIDIA is bejelentette, hogy foglalkozik a metaverzum kiépítésével.¹¹

A metaverzum előképének tekinthető élményekkel találkozhattak már bizonyos online játékok, így a Second Life vagy a Call of Duty használói, amelyek nagy részletességgel adják vissza a való élet körülményeit, és több játékos együttműködésén, kapcsolatán alapulnak.¹²

A metaverzum kiépítésének első fázisa az úgynevezett digitális ikrek (*digital twins*) létrehozása. Ebben a fázisban a fizikai világot leképezik egy virtuális világgá, tehát gyakorlatilag elkészül az eredeti másolata. A két világ, az eredeti és a másolat ekkor még teljesen párhuzamosan létezik egymás mellett. Másolat készül nem csupán a tárgyról, a fizikai valóságról, hanem az emberek is megjeleníthetők az új közegben. A science fiction művészet hagyományaihoz híven ezeket a virtuális lényeket avatároknak nevezik. Az avatár a hinduizmus kifejezése, olyan istenségeket jelöl, akik a földön emberi vagy állati formában küzdenek a gonosz ellen.¹³

A második fázisban a metaverzum már saját belső tartalmakat hoz létre – a használók, például az avatárok közreműködésével természetesen. A metaverzum alapját jelentő digitális közeg ekkor már nem csupán leképezése a való világnak, hanem annál több, illetve attól eltérő. Az új világ elkezd saját életét építeni, belső tartalmat (*native content*) hoz létre.

A harmadik, záró fázisban a két valóság egymással már teljesen összesimul, létrejön egy szürreális világ. A metaverzum végérvényesen magába zárja az eredeti világot, de már nem függ attól, önfenntartóvá válik.¹⁴ Nem ikrek már olyan értelemben, hogy a két világ nem tökéletesen azonos, még ha az összefüggések elkerülhetetlenek is, és a felhasználók értelemszerűen a való világból jelentkeznek be, és oda „lépnek vissza”.

A metaverzum felvonultat számos már ismert technológiát, amelyek hozzájárulnak majd a megfelelő működéshez, így például a mesterséges intelligencia, az Internet of Things, a biometrikus azonosítás,¹⁵ a Bluetooth vagy

¹⁰ Az európai adatvédelmi biztos TechSonar elemzése a metaverzumból: European Data Protection Supervisor: Metaverse.

¹¹ Disha Sinha: Top 10 Companies Working on Metaverse and Its Development in 2022. *Analytics Inside*, 2022. február 19. A szerző áttekintése szerint a tíz vállalat a következő: Meta, NVIDIA, Epic Games, Microsoft, Apple, Decentraland, Roblox Corporation, Unity Software, Snapchat, Amazon.

¹² Online: Second life; Call Of Duty.

¹³ Online forrás: Avatar. *Britannica*.

¹⁴ Yuntao Wang et al.: *A Survey on Metaverse: Fundamentals, Security, and Privacy*. 2022. 1–2.

¹⁵ A biometrikus azonosítók használata az elmúlt évtizedekben bővült. A bővülés mind a lehetséges azonosítási módok, mind a felhasználás volumenében megmutatkozik. Az egyelőre nem jósolható meg, hogy a biometrikus azonosítás kiszorítja-e majd a hagyományos azonosítási módokat, mindenestre a metaverzumban várhatóan jelentős szerepe lesz a biztonságosabb, de privacy szempontból érzékenyebb azonosítási módoknak. Vö. Szabó Endre Győző – Bojnár Katinka – Buzás Péter:

a blokklánc-technológiának is szerepe lesz az új virtuális világ fenntartásában.¹⁶ A belépési pontot egy virtuális valóságot közvetíteni képes szemüveg jelenti majd, így például a Microsoft Hololens¹⁷ vagy az Oculus.¹⁸ Az élmény teljességét szolgálják majd más, például a kezet megjelenítő és funkcióját biztosító eszközök vagy más szenzorok, kamerák, egyéb kellékek is. Mindezek azt eredményezik, hogy a felhasználó képes teljesen elmerülni a virtuális világban, teljes valójával annak részévé válik, érzékei és figyelme az offline világot gyakorlatilag teljesen kizárja. A szem és arc mozgását aprólékosan követő technológia a szemkontaktus lehetőségét ígéri, és valós idejű, a másik arcát, gesztusait közvetíteni képes közeget. Az emberi kommunikáció minél élethűbb közvetítése tehát alapvető kérdés a fejlesztések során.

A metaverzum adatvédelmi szempontú elemzése

Az alábbiakban a személyes adatok kezelésére és védelmére vonatkozó szabályok, illetve fogalommeghatározások segítségével elemezzük azokat a jogkérdéseket, amelyek bizonyosan meghatározói lesznek a metaverzum körüli adatvédelmi jogi problémáknak. A kérdések kiválasztásában a szerző hatósági tapasztalatai is szerepet játszottak. Számos olyan kérdés felvethető lenne, amelyek a már létező technológiai környezetben is releváns kérdések. Ezeket most figyelmen kívül hagyjuk, és a metaverzum újszerűségével járó problémákra koncentrálunk.

Személyes adatok az avatárok adatai?

A metaverzum kiépítésének első fázisában úgynevezett digitális ikrektől szóltunk feljebb. A koncepció kiindulópontja szerint mindennek és mindenkinek, aki részt kíván venni, meglesz a digitális leképezése az új közegben. Az emberek avatárok útján jelennek meg, ami azzal jár, hogy a hús-vér ember felhasználókhöz nem feltétlenül megszólalásig hasonló lények fogják képviselni őket az online világban. Ahogyan a virtuális játékokban, úgy a metaverzumban is elképzelhető, hogy az avatárok tulajdonságai alakíthatók lesznek. Ettől a lehetőségtől függetlenül a legfontosabb,

Új globális technológiák kihívásai a magyar jogban. In Tóth András (szerk.): *Technológia jog*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2016. 70–71.

¹⁶ A blockchain-technológia például a digitális ikrek védelmére szolgálhat. A blokklánc garanciaként szolgál arra, hogy a felhasználó a virtuális közegben nem egy megtévesztés áldozata, hanem amit lát, vagy akivel éppen kommunikál, az valóban az, aki, aminek tűnik. A sok felhasználó által használt felületen a bizalom megteremtése kulcskérdés, és ebben a blokklánc-technológia hatékony lehet. Vö. Ana Reyna et al.: On Blockchain and Its Integration with IoT. Challenges and Opportunities. *Future Generation Computer Systems*, 88. (2018), 173–190.

¹⁷ Online: Microsoft HoloLens.

¹⁸ Online: Oculus.

hogyan az avatár felismerhető lesz, még ha például a felhasználó „idealizált énjét” is fogja megjeleníteni.¹⁹

A szó technológiai értelmében az avatároknak is lesznek „adatai”, de ez valóban műszaki jellegű kérdés. A kérdés jogi oldala arra mutat rá, hogy függetlenül az avatárok és a felhasználók közötti hasonlóságtól, függetlenül a felhasználó által létrehozott avatárok számától, az adatok mindig köthetők lesznek egy természetes személyhez, akinek az adatvédelemhez való joga nem enyészik el.²⁰ Ennek megfelelően az avatárokhöz kötődő adatok személyes adatnak minősülnek a GDPR szerint.²¹

A személyes adatok elkísérik a metaverzumba is a felhasználókat, ennek megfelelően pedig az adatok védelmének igénye is elválaszthatatlan része marad a jogi követelményrendszernek. A metaverzum létrehozásán fáradozó piaci szereplők tisztában vannak ezzel az elvárással, illetve elvárásrendszerrel, ezért az új virtuális világ jellemzői között kiemelt helyen említik a privacy, illetve az adatok védelmét.²²

A természetes személy felhasználót képviselő avatár vagy avatárok (mert minden bizonnyal többet is létre lehet majd hozni) önálló életet élnek a virtuális közegben. Az avatárhoz kapcsolódó adatok végső soron a mögötte álló adatalany személyes adatainak tekintendők. Jogi értelemben nem tehetünk különbséget „valós” és „nem valós” adatok között, nem játszik szerepet az, hogy az avatár a természetes személy felhasználó életétől teljesen eltérő küllemmel és egyéb jellemzőkkel, magatartásmintákkal stb. jelenik meg a metaverzumban.

Adatvédelmi jogi szempontból csupán az a meghatározó, hogy ki a felhasználó, ki az adatalany, akit az érintetti jogok megilletnek. A virtuális személyiséggel összevetve ugyan „elszemélytelenedhet” az avatár, de az adatok jogi értelemben mindaddig személyesek maradnak, amíg a valós személlyel a kapcsolat kimutatható, akár közvetve, akár közvetlenül azonosítható marad. Az azonosíthatóság nem csupán a biztonságos üzemeltetés érdekében fontos, hanem az üzleti megfontolások

¹⁹ Szolin et al. (2023): i. m. 2., 10. Az interjúalanyok arról számoltak be, hogy a játékbéli avatárjuk tulajdonképpen egy kicsit az idealizált énjük is.

²⁰ A személyes adat jellegét megállapíthatjuk a tartalom elemzésével (ha az adat az érintettre vonatkoztatható), a célra tekintettel (az adat kezelésének célja, hogy az érintettet vagy az ő helyzetét befolyásolják), vagy az eredményre tekintettel (az adatkezelés hatással van az érintett érdekeire). Vö. Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ről*. Budapest, Wolters Kluwer Hungaria, 2018. 67–68.

²¹ A GDPR 4. cikk 1. pontjában rögzített „személyes adat” definíciónak az a kitétele, amely szerint a személy közvetlen vagy közvetett módon azonosítható, kétséget kizáróan érvényesül. Elképzelhető, hogy bizonyos személyek, illetve bizonyos adatok csak szűk adatkezelői kör számára lesznek hozzáférhetők, ez azonban nem változtat azon, hogy az érintett legalább közvetett módon azonosítható marad, és ezért rá a védelmi szabályok alkalmazandók.

²² A Meta által közzétett, Mark Zuckerberg szereplésével készült prezentáció is az elsődleges értékek között említi a biztonságot, az interoperabilitást, a nyitottságot és a privacyt. Online: The Metaverse and How We'll Build It Together – Connect 2021. *YouTube*.

is ebbe az irányba mutatnak. Legyen szó profilozásról, célzott reklámozásról, vagy bármilyen más üzleti értékről, a felhasználó környezetében keletkező adatok megőrzik személyes jellegüket.

Az adatvédelmi felelősség kérdései: adatkezelő és felhasználó – és akik közöttük vannak

A metaverzum „benépesítése” olyan vonzerőt igényel, amely meggyőzi a leendő felhasználókat arról, hogy valóban érdemes abban elmerülni és időt tölteni, valamint pénzt költeni a metaverzumban. Az élmény magával ragadó voltán túl a szolgáltatások megteremtésében, működtetésében részt vevő szereplők érdekalapon fognak dönteni arról, hogy belépjenek-e az új piacra. A közös érdek sok esetben közös adatkezelést fog eredményezni adatvédelmi jogi szempontból. Ez már a hagyományos piaci körülmények között is így volt, a metaverzum tehát a jelenlegi fogalomrendszerünkkel várhatóan nagy biztonsággal leírható lesz.

A szolgáltatói oldalon adatkezelőket fogunk tudni azonosítani, míg a felhasználó, ha szerepe nem terjed túl a hétköznapi használaton, a metaverzumban sem minősül sem adatkezelőnek, sem adatfeldolgozónak.²³ Ami bizonyosan megjósolható, hogy lesznek olyan felhasználók, akik egy másik szereplővel megvalósuló együttműködésük révén, így tipikusan reklámozás, profilozás céljából közös adatkezelői felelősséget fognak viselni.²⁴

A közös felelősség kérdéseit az Európai Unió Bírósága több döntésében is elemezte, és kimondta, hogy az egyszerű felhasználó nem válik a Facebookkal együtt felelőssé a személyes adatok kezeléséért, azonban a rajongói oldal (*fan page*) adminisztrátora nem egyszerű felhasználó. Ami a különbségtételt indokolja, az a Wirtschaftsakademie-ügyben született ítélet szerint az, hogy a rajongói oldal létrehozója lehetővé teszi a Facebook számára, hogy az oldal látogatóinak számítógépén cookie-kat helyezzen el. Az adminisztrátornak beállításokat kell eszközölnie az oldalon, ami befolyásolja a személyes adatok kezelését. Összességében tehát az adminisztrátor részt vesz a személyes adatok kezelése céljának és módjának meghatározásában, tehát ő is adatkezelőnek tekintendő.²⁵

Ha az elemzés nem is lehet teljes, minden részletre kiterjedő egyelőre, de a jelenlegi ismereteinkkel azt már előre tudjuk jelezni, hogy az egyes szereplők

²³ Az Európai Unió általános adatvédelmi rendelete, a GDPR (18) preambulumbekzdése szerint személyes vagy otthoni tevékenységnek minősül többek között a közösségi hálózatokon történő kapcsolattartás és az online tevékenységek. Az „átlagos” felhasználó tehát adatvédelmi felelősséget nem visel általánosságban, és ezt a privilegiált helyzetét a metaverzumban is meg fogja őrizni.

²⁴ A C-210/16. sz. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein kontra Wirtschaftsakademie Schleswig-Holstein ügyben hozott előzetes döntés 35–41. pontjai szerint. Hasonló adatvédelmi jogi elemzést végez el az EUB a Planet 49 (C-673/17), a Fashion ID (C-40/17) és a Jehova Tanúi (C-25/17) ügyekben hozott döntéseiben.

²⁵ A Wirtschaftsakademie ügyben született ítélet (39) pontja.

az adatvédelmi jogi minőségüket a metaverzumban is meg fogják őrizni, ahogyan azt a hagyományos piaci körülmények között megszerezték.

Az Európai Unió Bírósága a védelem megerősítése érdekében az adatkezelői felelősség minél szélesebb körű alkalmazását fontosnak tartotta a közös adatkezelői felelősséget elemző döntéseiben.²⁶ Ez a megközelítés a jogalkalmazás minden területén figyelembe veendő. Bár a metaverzum kínálhat majd újszerű üzleti modelleket, a jogértelmezésben az a tendencia, hogy az adatkezelői felelősséget minél szélesebb körben kell megállapítani, az új virtuális környezetben is irányadó marad. Feltételezhető az is, hogy a metaverzum az összetettebb adatkezelések révén több lehetőséget kínál majd az olyan kooperációkra, amelyek esetében a fent elemzett ítéletek alapján a közös adatkezelői felelősség megállapítható lesz.

*Önkéntelenség, teljes beolvadás, az ösztönös védelmi mechanizmusok
kikapcsolása – a kockázatok megbecsülésére tett kísérlet*

A metaverzum mögött álló mesterséges intelligencia személyre szabott szolgáltatásokat képes létrehozni. Az MI-algoritmusok gazdag és személyes élményvilágot fognak teremteni, termékek, szolgáltatások, információk ajánlásával.²⁷ A technológia tehát készen áll a metaverzum élményekkel való feltöltésére, és ezzel a képességével az adatvédelmi elemzés során is számolni kell.

Mi teszi kockázatosabbá magánszféra-védelmi szempontból a metaverzumot a korábbi technológiai megoldásoknál? A teljes belemerülés, belefeledkezés jelenségét kell itt elsősorban megemlíteni. Akkor, amikor a felhasználó „fél lábbal” kívül áll a virtuális világon, másik felével pedig az online környezetben van, csak egyfajta korlátozott virtuális élményről beszélhetünk. A felhasználó például kezében tartja a telefont, hallja a külvilágból származó hangokat, érzékeivel alapvetően nem a virtuális világ része, hanem az offline-é.

A metaverzum elképzelt világába érkezve a felhasználó teljes valójával a virtuális világba lép be, ott gyakorlatilag feloldódik az őt fogadó környezetben. Bár a felhasználónak értelemszerűen lesz lehetősége alakítani saját környezetét (ennek részletei majd a tényleges megvalósulás időszakában tisztázódnak), és ő maga irányíthatja majd a navigálás menetét, mégis folyamatosan ki lesz téve előre nem látható élményeknek, választási lehetőségeknek.

Könnyen elképzelhető olyan helyzet, amikor érzékeny döntési helyzetbe kerül, akár világnézeti, akár például politikai jellegű választás elé áll az avatárja révén a gyanútlan felhasználó. Az adott ország kultúrájától, szokásaitól, aktuális közéleti eseményeitől függően egészen apró gesztusok, hétköznapiak tűnő preferenciák

²⁶ Szabó Endre Győző: *A védelmi lépcső elmélete*. Budapest, Ludovika Egyetemi Kiadó, 2022. 79–80.

²⁷ Wang et al. (2022): i. m. 7.

is politikai, világnézeti állásfoglalásként foghatók fel, vagy más véleményre engedhetnek következtetni. Ezeket az adatokat aztán sokféleképpen lehet elemezni, felhasználni.²⁸

Nem szabad elfelejteni, hogy az online viselkedés mindig jól monitorozható, visszakereshető, ezért a metaverzum a maga steril formájában a magánszféra el-lentéteként írható le. A világháló előtti kitárulkozás és a folyamatos megfigyeltség lehetősége egy nemkívánatos kombináció: tökéletes ellentpntja annak az állapotnak, amelyet magánszféra-védelmi szempontból ideálisnak tartunk, nevezetesen a más által nem zavart létezés, amelyben az ember úgy viselkedhet, ahogyan neki jólesik, és a személyiség úgy bontakozhat ki, ahogyan azt egészségesnek tekintjük.

Az említett választási kényszerhelyzet, mint a megnyilvánulás elkerülhetetlen példája értelemszerűen csak egy a sok lehetséges és elképzelhető szituáció közül. Az online közegben kialakult gyakorlatokat és súlyos visszaéléseket figyelembe véve naivitás lenne azt állítani, hogy ilyen helyzetek nem adódhatnak, illetve adott esetben ezek megteremtése mögött ne állhatna tudatosság. Az ilyen helyzetek megteremtésében az eredetire megszólalásig hasonlító úgynevezett *deep fake* másolatok is szerepet játszhatnak, illetve a manipuláció egyéb formái, mint a sürgetés, pszichológiai nyomás, félelemérzet keltése. Ezzel a kockázattal tisztában kell lenni, és a felhasználónak egészséges bizalmatlansággal kell majd bejárnia a metaverzum helyszíneit.

Készülni is lehet a kockázatokra, ebben a technológiai megoldások is a felhasználó segítségére lehetnek. Az avatárt át lehet vinni egy olyan környezetbe, amely a metaverzum egy adott szegmensének másolatából készül, ahol a felhasználó magára maradhat, és nem lehet lehallgatni. Vagy például láthatatlanná lehet tenni az avatárt mások számára, és ennek révén előzhető meg a visszaélések.²⁹ Az egy másik kérdés, hogy amennyiben az avatárok egymás számára láthatatlanná tehetők, és ezt a felhasználók tömegével meg is fogják tenni, akkor a metaverzum mennyiben jeleníti majd meg azt a közeget, amelyet a fejlesztők megálmodtak.

Az érzelmi reakciók feltérképezése

A felhasználó érzékeny területeket érintő véleményéhez hasonlóan az érzelmi reakciók elemzése szinte korlátlan távlatokat nyit a különböző preferenciák

²⁸ Az osztrák adatvédelmi hatóság 2019 októberében az osztrák postára vetett ki 18 millió eurós összegű bírságot. Az osztrák hatóság úgy ítélte meg, hogy a posta birtokába kerülő, a lakosok politikai hovatartozására is következtetni engedő információk nem használhatók a „politikai affinitás” megismerésére, továbbá az ilyen információk értékesítése nem áll összhangban az adatvédelmi szabályozással. Bár a határozatot az osztrák közigazgatási bíróság formai okokból hatályon kívül helyezte, a bíróság is megerősítette az adatkezelés jogellenes voltát. Online: BVwG–W258 2227269-1/14E.

²⁹ Wang et al. (2022): i. m. 40.

megfigyelésére. Itt is emlékeztetni kell arra, hogy a metaverzum azt az élményt ígéri, hogy tulajdonképpen teljes beleolvadást hoz magával, és egy valóságosnak tűnő, másodlagos világot teremt. Ebben a felhasználó egy ponton túl már nem képes „viselkedni”, hanem önmagát adja, minden tekintetben önkéntelenül cselekszik. A családtagok, barátok jelenléte, a magával ragadó felhasználói környezet ebben az aspektusban teljesen védtelenné teszi az avatar mögött húzódó tényleges felhasználót az esetleges megfigyeléssel, profilozással szemben.

A metaverzum futurisztikus világában a felhasználó szociális helyzetek résztvevője lehet majd, akár ismerősökkel, akár ismeretlenekkel találkozva. A felhasználó ezekben a helyzetekben valószínűleg hasonlóan fog viselkedni, mint az offline közegben. Ezt a megállapítást azzal is alátámaszthatjuk, hogy a felhasználók nagy része a közösségi kapcsolataik kibontakoztatásának lehetőségét látják majd a metaverzumban, ezért nem fognak majd „kettős életet” élni. A kisebbség ettől eltérő magatartása nem változtatja meg az elemzésünk alapjait.

Ezt az okfejtést támasztja alá az a tilburgi elemzés, amely a Second Life-felhasználók viselkedését vizsgálta. Igaz, hogy a felhasználók önbevallására alapozott a kutatás, és itt torzíthatnak az adatok,³⁰ de a kutatás következtetésként azt vonja le, hogy amennyiben a virtuális világban valóságos társadalmi interakciók zajlanak le, akkor ez lehetőséget ad a valós társadalmi kapcsolatok feltérképezésére, elemzésére is.

Az érzelmi reakciók, illetve általában az érzések megjelenítése az online közegben mindenképpen egy fontos határ átlépését jelenti. Az adatvédelmi hatóságok is jelentőséget tulajdonítanak ennek, különösen, ha az érintett számára nem észlelhető módon történik, akár a bűnüldözés területén,³¹ vagy üzleti típusú felhasználás esetén.³²

³⁰ Ronald Leenes: Privacy in the Metaverse. Regulating a Complex Social Construct in a Virtual World. In Simone Fischer-Hübner – Penny Duquenoy – Albin Zuccato – Leonardo Martucci (szerk.): *The Future of Identity in the Information Society*. Boston, MA, Springer, 2008. 100–101.

³¹ Az Európai Adatvédelmi Testület 5/2022. számú, az arcfelismerő technológia használatáról a bűnüldözés területén címet viselő iránymutatása több olyan, a magánszférába súlyosan beavatkozó felhasználási módot említ, amelyekre tilalmat javasol. Az egyik ilyen az olyan arcfelismerő technológia, amely a természetes személyek érzelmeire nézve képes következtetéseket levonni. Online: Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement. 5.

³² A Nemzeti Adatvédelmi és Információszabadság Hatóság NAIH-85-3/2022 számú határozatában egy bank felelősségét állapította meg telefonos ügyfélszolgálati munkatársakkal folytatott, rögzített beszélgetések elemzése kapcsán. A határozat szerint „[a]z Ügyfél az elemzés eredményét felhasználva állapítja meg, hogy melyik elégedetlen ügyfelet szükséges visszahívni, ezzel kapcsolatban többek között automatikusan elemzi mind a telefonáló érintett, mind az ügyfélszolgálati munkavállaló érzelmi állapotát és a beszélgetés egyéb jellemzőit”. Az ügyben a hatóság mind ez idáig legmagasabbnak számító, 250 millió forintos bírságot szabott ki, ezzel is aláhúzza a jogsértés súlyát és az adatkezelés tolakodó jellegét.

A fogyasztó által generált adatok kiszámíthatatlansága tehát megbecsülhetlenné teszi a lehetséges kockázatokat is. A kockázatalapú megközelítést alkalmazó adatvédelmi szabályozással kapcsolatban itt a metaverzum egy jelentős és további vizsgálatot, garanciákat követelő jellemzőjére kell rámutatnunk.

Az egészséges mértékű internethasználat és a magánszféra összefüggéséről

Az internet használatával összefüggésben nem csupán azokról a kockázatokról tudunk, amelyek a felhasználóra leselkednek, hanem önmagában a túlzott mértékű, túl hosszú használatot is megemlítjük a metaverzum elemzése kapcsán. A metaverzum természeténél fogva magában hordozza azt a lehetőséget, hogy a felhasználói élmény fokozása révén az interneten töltött idő meg fog növekedni. Minél jobban összeolvad a magánszféra és a virtuális közeg, annál valószínűbbnek tűnik, hogy ez ténylegesen bekövetkezhet. A magánszféra határait és meghatározó élményeit befolyásoló közeg kapcsán felmerül a kérdés, hogy a viselkedési minták változásával nő-e a kockázata az úgynevezett viselkedési addikcióknak.

Ahogy Bányai Fanni és szerzőtársai fogalmaznak, „[f]üggő magatartásról akkor beszélhetünk, ha a viselkedés uralni kezdi az egyén életét, károsítja annak és környezetének testi-lelki állapotát”.³³ A pszichológusszakma arra mutat rá, hogy függőséget nem csupán például valamilyen kémiai jelenség okozhat, hanem zavarhoz vezethet bizonyos magatartások túlzásba vitele, és a normális magatartás már nem okoz megelégedettséget, az egyén élete kibillen korábbi egyensúlyából. Nem azt állítom, hogy a metaverzum vegytiszta megvalósulása esetén automatikusan adódik a felhasználók széles tömegét érintő, fent leírt kockázat. Azt a következtetést ugyanakkor megalapozottan vonhatjuk le, hogy a felhasználók kisebbségét érintő úgynevezett problémás internethasználat³⁴ egy új dimenzióval fog kiegészülni.

A természetes közegben megélhető és megelégedést nyújtó magánszféra ebben a kontextusban nem csupán védelmet élvező és védendő közegként írható le, hanem úgy is, mint a magatartási addikció ellen ható, a normális magatartást megjelenítő, végső soron az egyént és az ő társas kapcsolatait védő környezet. Használhatnánk a „buborék” kifejezést, akár figyelmeztetésként is, hogy a túlzott internethasználat ellenében a magánszféra jelentőségét hangsúlyozzuk. Ez ugyanis az a közeg, amelyben a személyes adataink elsődlegesen keletkeznek.

Az elemzésünk arra mutat rá, hogy helyes az a törekvés, ha magánszféránk minél kisebb részét jelenítjük meg az online világban, és az ott töltött idő is korlátozás alá

³³ Bányai Fanni et al.: A problémás videojáték-használat újabb elméleti és gyakorlati megközelítései. *Információs Társadalom*, 18. (2018), 1. 93–106.

³⁴ A problémás internethasználat (Problematic Use of the Internet, PUI) számos jelenséget foglal magában, így játékkal, szerencsejátékkal, online zaklatással kapcsolatos problémákat. Vö. Learning to Deal with Problematic Usage of the Internet. *COST – European Cooperation in Science and Technology*.

esik. Az online és offline világ összefonódásából előálló metaverzumban minden bizonnyal még nehezebb lesz ezt megvalósítani. Az sem idegen gondolat a közösség szintjén, ha a virtuális közegben is elérhetőek bizonyos információk, adott esetben támogatás azok számára, akik a függőségből keresnek kiutat. Ezen a ponton viszont már olyan mélyen járunk a való és virtuális világ összefonódásában, hogy messze eltértünk a szűk értelemben vett adatvédelmi elemzéstől. Mégsem haszontalan elkalandozás ez, hiszen jól illusztrálja az új technológiával kapcsolatos kérdések sokaságát és megválaszolatlanságát.

Fizikai távolság

Képzavarnak tűnhet a metaverzumról szóló tanulmányban fizikai távolságról írni. A felvetés azonban semmiképpen sem indokolatlan, mert az avatárok mögött hús-vér emberek állnak, akik a magánszféra iránti igényüket megőrzik a virtuális világban is. Ott sem tolerálják a bizonyos határt átlépő közelséget. Nem sokkal a létrejötte után a virtuális valóságra épülő közösségimédia-platfommon, a Horizon Worlds felületén történt szexuális zaklatásról számolt be az egyik női felhasználó.³⁵ Úgy tűnik, hogy a virtuális világ sem óv meg azoktól a jelenségektől, amelyekről az offline világban is szabadulnánk.

Továbbá azért sem indokolatlan a fizikai közelség témájáról szólni, mert a metaverzum egyfajta leképeződése a valóságos világnak, és a magánszférára, a mások által meg nem zavart térre ott is szükség van. Nem őrizhető meg a virtuális világ sem élhetőnek, élvezhetőnek, ha nem áll rendelkezésre olyan eszköz, amely a személyes tér kikényszerítését szolgálja.³⁶ A magánszféra klasszikus szabályai az online térben is helyet követelnek maguknak. A Meta úgy reagált a felhasználói igényekre, hogy minden avatárt egy két láb sugarú (körülbelül 60 cm) virtuális kör vesz körül, ami végső soron azt eredményezi, hogy a felhasználók nem kerülhetnek négy lábnál közelebb egymáshoz.³⁷ Ilyen módon próbálják elkerülni a kellemetlen vagy tolatkodó élményeket, és az egészséges fizikai távolságra szorítani azokat, akik ezt zaklató módon át szeretnék lépni.

A fizikai távolság kapcsán nem újdonság, amiről itt értekezünk. Az intim, a személyes, a társadalmi és a nyilvános kapcsolatokhoz tartozó egészséges távolság meghatározása a pszichológia tudományának művelőit már régóta foglalkoztatta.

³⁵ Tanya Basu: The Metaverse Has a Groping Problem Already. *MIT Technology Review*, 2021. december 16.

³⁶ Lásd ebben a tekintetben a privacy jogának alapjait megfogalmazó szerzőpáros tanulmányát: Louis D. Brandeis – Samuel D. Warren: The Right to Privacy. *Harvard Law Review*, 4. (1890), 5. 193–220.

³⁷ Kyle Orland: Meta Established 4-Foot 'Personal Boundary' to Deter VR Groping. *Ars Technica*, 2022. július 2.

G. Stanley Hallnak tulajdonítják ezt a felosztást, amely pontosan meg is határozta ezeket a határokat.³⁸ Hall is körülbelül 50 centiméteres távolságot jelölt meg az intim kör határaként.

Adatbiztonsági kockázatok és megfontolások

A metaverzumot ebben a tanulmányban új technológiaként írjuk le. Amint láttuk, sok tekintetben nem teljesen új, hanem a már létező technológiák újszerű kombinációjaként is leírható. Ennek megfelelően számos adatbiztonsági kockázat nem teljesen ismeretlen, így a felhasználó azonosításához kapcsolódó kockázatok, az identitáslopás, a megtévesztő megismerésével járó visszaélések, az avatar azonosításához kötődő visszaélések olyan jelenségek, amelyek a metaverzum nélkül is felmerülnek.

Közelebb a felhasználóhoz

A metaverzum olyan mértékű adatgyűjtést és adatkezelést vetít előre, amely minden korábbi felhasználói környezet adatigényét felülmúlja. Kézenfekvőnek tűnik a felhőszolgáltatások igénybevétele, amelyek rugalmas háttérrel biztosítanak az új virtuális világ fenntartásához. A hatalmas mennyiségű és adott esetben érzékeny információ felhőben való tárolásának jelentős kockázatai vannak. Az adatok felhasználói eszközökön való tárolása mind biztonsági, mind magánszféra-védelmi megfontolásokból helyesebb választás lenne.³⁹ Így például a szem mozgására vagy a testmozgásra vonatkozó adatok nem a felhőben, hanem a felhasználó eszközén lennének elérhetők. Ilyen módon elejét lehetne venni az incidensekből fakadó problémáknak, továbbá az adatokkal való egyéb visszaéléseknek.

Jogtalan hozzáférés az adatokhoz

Bár az adattakarékosság elvét az adatkezelőre vonatkozó kötelezettséggé tartjuk számon, a felhasználó szempontjából is van jelentősége.⁴⁰ A felhasználó úgy tudja a lehetséges kockázatokat csökkenteni, ha valóban a szükségesre szorítja

³⁸ Wang et al. (2022): i. m. 18. Négy fizikai távolságot azonosított: a nyilvános térben 3,5–7,5 métert, a társasági térben 125–350 centimétert, a személyes körben 50–125 centimétert, míg az intim terület határát 50 centiméteres távolságban.

³⁹ Az úgynevezett *edge computing* gyakorlatilag a felhasználóhoz lehető legközelebbi adatfeldolgozást jelenti, amelynek adatbiztonsági mellett üzleti előnyei is kiaknázhatók.

⁴⁰ A GDPR 5. cikk (1) bekezdés c) pontja szerint a kezelt személyes adatoknak az adatkezelés céljai szempontjából megfelelőeknek és relevánsnak kell lenniük, és a szükségesre kell korlátozódniuk.

az internethasználatot, valamint az annak során feltárt információkat. Ez a megállapítás nem új, de az új technológia vizsgálatakor mégis új jelentőséggel bővül a tartalma.

A virtuális világban nem mindent és mindenkit képes észlelni a felhasználó. Előfordulhat, hogy egy álcázott formában megjelenő felhasználó (avatár) megfigyeli a felhasználó magatartását vagy egy csoport magatartását. Az is lehetséges, hogy a való életről megfélelmett felhasználó fizikai közelségében lévő másik személy képes a beszélgetést, kommunikációt kihallgatni. Az első esetben megoldást nyújthat, ha több avatárt készít a felhasználó, és a rosszindulatú kémkedőkkel szemben megtévesztő stratégiát alkalmaz.⁴¹ Ami a fizikai életben való biztonságot illeti, ott arra kell figyelmeztetni, hogy a teljes belemerülést kínáló metaverzum használatának helyét jól meg kell tervezni, és az illetékteleneket fizikailag is ki kell zárni onnan.

Összegzés

A metaverzum egy sok tekintetben futurisztikus és lenyűgöző virtuális világot kínál, amelyben a felhasználó újszerű módon lesz képes feloldódni a digitális környezetben. A fenti elemzésben arra jutottunk, hogy az új technológia csak részben vet fel újszerű adatvédelmi kérdéseket. A magánszférát érintő szempontokon túl néhány olyan kérdést is elemeztünk röviden, amelyek csupán illusztrációi a metaverzumot, valamint általában az internethasználatot érintő társadalmi kérdések sokaságának.

A metaverzum előképei már léteznek, a virtuális valóságban zajló játékok tapasztalatai sok mindent előrevetítenek abból, ami a metaverzumot a jövőben jellemezni fogja. Az új virtuális közeg semmiképpen sem lesz jogon kívüli terület, ott sok más követelmény mellett az adatvédelmi szabályozás is érvényesítendő lesz. A metaverzum a magánszférát sok szempontból érinteni fogja. Az avatárokhöz kapcsolódó adatokat személyes adatnak kell tekinteni, amelyek védelme érdekében intézkedéseket kell majd tenni. Különös jelentősége lesz a *privacy by design* elvnek a rendszer tervezése során.

Az adatkezelők várhatóan sok esetben osztozni fognak az adatkezelői felelőségen más adatkezelőkkel, és a közös adatkezelői minőség minden bizonnyal számos üzleti modellben érvényesülni fog. Az adatalanyok önkéntelenül is sok személyes adatot fognak feltárni magukról a metaverzumban. Az ilyen adatok kezelését a lehető legszűkebbre kell visszaszorítani, így a különleges adatkategóriába tartozó adatokét, vagy például a felhasználók érzelmi reakcióit leíró adatokat.

Ahhoz, hogy a metaverzumban a magánszféra megőrizhető legyen, a tervezés során védelmi funkciókat kell beépíteni. Ilyen a fizikai távolságot szimuláló funkció,

⁴¹ Lik-Hang Lee et al.: *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*. (2021).

de sok más intézkedést kell elérhetővé tenni, például a mások figyelmé előli elvonulásra lehetőséget adó megoldásokat.

A klasszikus adatbiztonsági problémák a metaverzumban is jelen lesznek. A hozzáféréskontroll érzékeny kérdéseket vet fel, hiszen a biometrikus azonosítók adott esetben magasabb biztonságot képviselhetnek, míg a kezelésük önmagában is magas kockázatúnak tekintendő. Az idő mutatja majd meg, hogy a felhasználók e tekintetben milyen megoldásokat részesítenek előnyben.

A tanulmány fontos kérdéseket vetett fel, és mutatott be néhányat vázlatosan. Más következtetést nem tudunk levonni, mint hogy a metaverzum jogi és magánszféra-védelmi kérdései terén számos további kutatásra lesz szükség a társadalmi hatások pontos feltérképezéséhez.

Felhasznált irodalom

- Bányai Fanni – Zsila Ágnes – Demetrovics Zsolt – Király Orsolya: A problémás videojáték-használat újabb elméleti és gyakorlati megközelítései. *Információs Társadalom*, 18. (2018), 1. 93–106. Online: <https://doi.org/10.22503/infars.XVIII.2018.1.6>
- Basu, Tanya: The Metaverse Has a Groping Problem Already. *MIT Technology Review*, 2021. december 16. Online: www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/
- Brandeis, Louis D. – Samuel D. Warren: The Right to Privacy. *Harvard Law Review*, 4. (1890), 5. 193–220. Online: <https://doi.org/10.2307/1321160>
- Lanier, Jaron: *You Are Not a Gadget*. London, Penguin Books, 2011.
- Leenes, Ronald: Privacy in the Metaverse. Regulating a Complex Social Construct in a Virtual World. In Simone Fischer-Hübner – Penny Duquenoy – Albin Zuccato – Leonardo Martucci (szerk.): *The Future of Identity in the Information Society*. Boston, MA, Springer, 2008. 95–112. Online: https://doi.org/10.1007/978-0-387-79026-8_7
- Lee, Lik-Hang – Tristan Braud – Pengyuan Zhou – Lin Wang – Dianlei Xu – Zijun Lin – Abhishek Kumar – Carlos Bermejo – Pan Hui: *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*. 2021. Online: <http://doi.org/10.13140/RG.2.2.11200.05124/8>
- Orland, Kyle: Meta Established 4-foot ‘Personal Boundary’ to Deter VR Groping. *Ars Technica*, 2022. július 2. Online: <https://arstechnica.com/gaming/2022/02/meta-establishes-four-foot-personal-boundary-to-deter-vr-groping/>
- Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer Hungary, 2018.
- Reyna, Ana – Cristian Martín – Jaime Chen – Enrique Soler – Manuel Díaz: On Blockchain and its Integration with IoT. Challenges and Opportunities. *Future Generation Computer Systems*, 88. (2018). 173–190. Online: <https://doi.org/10.1016/j.future.2018.05.046>
- Sinha, Disha: Top 10 Companies Working on Metaverse and Its Development in 2022. *Analytics Inside*, 2022. február 19. Online: www.analyticsinsight.net/top-10-companies-working-on-metaverse-and-its-developments-in-2022/
- Szabó Endre Győző: *A védelmi lépcső elmélete*. Budapest, Ludovika Egyetemi Kiadó, 2022.

- Szabó Endre Győző – Bojnár Katinka – Buzás Péter: Új globális technológiák kihívásai a magyar jogban. In Tóth András (szerk.): *Technológia jog*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2016. 51–97.
- Szolin, Kim – Darija J. Kuss – Filip M. Nuyens – Mark D. Griffiths: “I Am the Character, the Character Is Me”: A Thematic Analysis of the User-Avatar Relationship in Videogames. *Computers in Human Behaviour*, 143. (2023). Online: <http://dx.doi.org/10.1016/j.chb.2023.107694>
- Westin, Alan F. (szerk.): *Information Technology in a Democracy*. Cambridge, MA, Harvard University Press, 1971.
- Wang, Yuntao – Zhou Su – Ning Zhang – Rui Xing – Dongxiao Liu – Tom H. Luan – Xuemin Shen: *A Survey on Metaverse: Fundamentals, Security, and Privacy*. 2022. Online: <https://doi.org/10.48550/arXiv.2203.02662>

Intézményi dokumentumok

- European Data Protection Supervisor: *Tech Sonar 2022–23 report*. Online: https://edps.europa.eu/system/files/2022-11/22-11-10_techsonar_report_22_23_en.pdf
- European Data Protection Supervisor: *Metaverse*. Online: https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en

Online források

- GDPR Hub. Online: https://gdprhub.eu/index.php?title=BVwG_-_W258_2227269-1/14E
- Snow Crash Summary and Study Guide. *SuperSummary*. Online: www.supersummary.com/snow-crash/summary/
- Neal Stephenson on the Future of the Metaverse. *YouTube*. Online: www.youtube.com/watch?app=desktop&v=60u9L5-YO9Q
- Próteusz. *Arcanum*. Online: www.arcanum.com/hu/online-kiadvanyok/Lexikonok-ki-kicsoda-az-antik-mitoszokban-F869D/p-F8BBC/proteusz-F8C7E/
- Proteus effect. *Tech Target*. Online: www.techtarget.com/whatis/definition/Proteus-effect#:~:text=The%20Proteus%20effect%20is%20the,accordance%20with%20their%20digital%20representatives
- Metaverse. *European Data Protection Supervisor*. Online: https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en
- Avatar. *Britannica*. Online: www.britannica.com/topic/avatar-Hinduism
- The Metaverse and How We'll Build It Together – Connect 2021. *YouTube*. Online: www.youtube.com/watch?v=Uvufun6xer8
- Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement. Online: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf
- Learning to Deal with Problematic Usage of the Internet. *COST – European Cooperation in Science and Technology*. Online: www.cost.eu/publication/learning-to-deal-with-problematic-usage-of-the-internet/