Kriskó Edina

Új kihívások a virtuális és a kiterjesztett valóságok korában

E tanulmány a virtuális és a kiterjesztett valóságok világába vezeti el az olvasót. Teszi mindezt azért, hogy rávilágítson néhány olyan új kihívásra és visszaélési módra, amelyet számos professzió kénytelen mérlegre tenni a kommunikációtól a rendészetig bezárólag. A vizsgált tárgykör e percben még sem a jogtudomány, sem a rendészet számára nem a mainstream kutatási vonalat jelenti, (bár eredetileg rendészeti kommunikációs kutatásnak indult a felderítés,) de napirendre tűzésével már nem sokáig késlekedhetünk. A fő kérdésünk: mi történik velünk, az emberrel a közvetített valóságokban, sérülékenységünk milyen új dimenziói nyíltak meg, s milyen jelenségekről kell közösen – multi- és interdiszciplináris közelítésben – gondolkodnunk. Megváltozott a cyberbűnözés jellege és színtere, folyton változásban van a *privacy* fogalma, ahogyan változunk mi magunk és az a kulturális közeg is, amelyben egyre jobban átszövi életünket a technológia, a mediatizált környezetek, a megfigyelés. Már csak egy lépés a transzhumán lét, ideje tehát megnézni, milyen irányba haladunk…

Bevezetés

Avatarok,[1] fiktív profilok, a való (offline) életben sosem létezett (online) barátok, virtuális közösségek, gombnyomásra elkövetett bűnök és digitális lábnyomok *(digital footprint):* csak néhány azon jelenségek közül, amelyeket a digitalizáció, az internet és a közösségi média vagy a mediatizált valóságok hoztak el az életünkbe. Hackerek és crackerek, fehér és fekete kalaposok[2] és az úgynevezett szürkezónában mozgó felhasználók,[3] anonymusok, akik a társadalmi-gazdasági kontroll megtestesítőiként lépnek színre az online térben – megannyi fogalom, amelyet nemrégiben tanultunk. Ismerkedünk a hálózati logikával, a participáció élményével, a megfigyelés és a felügyelet kultúrájával, önmagunk, képességeink és világunk kiterjesztésével, transzformálásával, az emberi lét meghaladásával a mesterséges intelligencia és az okoseszközök által. Egy új – bűnöktől és bűnözéstől sem mentes – univerzum (vagy sokkal inkább metaverzum) született, a közvetített valóságok korába léptünk. A rendészeti szakma a mélynet sötét titkait kutatja, maszkolt identitások[4] és anonim aktorok, illegális cserefolyamatok között keresi önnön funkcióit és digitális identitását, kutatja cselekvési kompetenciája határait.

1 A személyiség digitális vagy virtuális kivetülése, amely akár fiktív elemeket is tartalmazhat. A kommunikációelmélet által homlokzatnak nevezett kép, amelyet a felhasználó másoknak mutat, illetve amilyennek mások számára az online, illetve virtuális térben mutatkozik. Az avatar a hindu vallásból kölcsönzött kifejezés, amely eredetileg testet öltést jelent. Egy szellemi lény vagy istenség megjelenése ember vagy állat alakjában („aki alászáll"). Az internetes közösségekben a képmás, a profil, a virtuális világokban valamilyen háromdimenziós objektum (www.sztaki.hu). Az avatar szecenáriófüggő megválasztásáról lásd még: WU, Jennifer: Choosing My Avatar & the Psychology of Virtual Worlds: What Matters?, *Kaleidoscope*: Vol. 11, Article 89., 2013., http://uknowledge.uky.edu/kaleidoscope/vol11/iss1/89 (utolsó letöltés: 2016.VI.01.).

2 A fehér kalaposok *(hackerek)* megbízás alapján tárnak fel biztonsági réseket, a fekete kalaposok *(crackerek)* törvénytelen informatikai támadások végrehajtói.

3 Akik időnként átlépik a határokat, szabályokat (jogi értelemben).

4 Az az arc (álarc), amelyet a felhasználó másoknak mutat magáról az online térben, mikor hozzáférhetővé teszi bizonyos tulajdonságait (például nemét, korát, preferenciáit, adottságait), és a tulajdonságok egy részét (például kommunikációs stílusát) önkéntelenül fedi fel.

Új fegyver jelent meg a hagyományos rendészet ellenében, a magasszintű IT tudás, a *mélynet*[5] és a *hacktivizmus*[6] románcából született antiutópia, a bármikor bárhonnan elkövethető visszaélések eszköze, a *cyber crime* megannyi mindennap bővülő-változó formája.

E tanulmány nem vállalkozik mindezek áttekintésére, hiszen könyvtárnyi kérdést kellene tisztázni. Pusztán arra tesz kísérletet, hogy ízelítőt nyújtson – kissé technológiai determinista alapokon – a biztonság új típusú, virtuális valóságokhoz kapcsolódó kihívásaiból. Üzenete az, hogy a rendészetnek szemléletében kell elsősorban felzárkóznia a felhasználók által mind nagyobb arányban használt kommunikációs színterek logikájához. A rendészeti szakmának – és nem csak a kiberbűnözés specialistáinak – széles körben meg kell ismernie, hol is időznek polgárai, kommunikációs aktusaik milyen mélyreható változásokat (olykor károkat) idéznek elő testben és szellemben, érzelemben és identitásban, mik a visszaélések új és jövőbeni formái, amelyek egy részéről még csak találgatunk.

Kiberbűnözés: a kezdetektől a kiberterrorizmusig

A számítógépes bűnözés kezdeteit a mai napig homály fedi. Fennmaradt ugyan néhány esetleírás, anekdota és legenda, de a források hiányosak. Annyi azonban bizonyosnak tűnik, hogy a visszaélésekkel szembeni aggodalmakat a számítógépet használó cégek könyvelői és auditorai artikulálták elsőként valamikor az 1950-es és az 1960-as években (főként annak köszönhetően, hogy alapvető információknak is híján voltak a számítógépes pénzügyi elszámolások programozási alapjait illetően) (Cortada 2008). Sokáig a kiberbűnözés fogalma is tisztázatlan maradt. A hatóságok egy része úgy fogalmazott: „számítógép használata nagy pénzösszegek ellopására";[7] más részük azt vallotta: „szolgáltatások ellopása, beleértve a definícióba a személyiségi jogok megsértését is",[8] olyan hatósági álláspont is akadt, amely szerint: „számítógép használata bármely rendszer megtévesztésére mások forrásainak, szolgáltatásainak és tulajdonának megsértése céljából" (uo.).[9]

1983-ban már közmegegyezés övezi, hogy idesorolható a hardverek és a szoftverek rongálása *(vandalism)*, az információlopás, a hardverlopás, a szoftverlopás, a szoftverek vagy fájlok megváltoztatásával elkövetetett pénzügyi csalás vagy lopás, a szolgáltatások jogtalan használata vagy eladása számítógép használatával (uo.). Nagyjából erre az időre datálható a szervezett bűnözés megjelenése a cybertérben, amelynek kulcsterületei a szerencsejáték (online fogadóirodák), a prostitúció és a pornográfia, a kábítószer-kereskedelem, a feketekereskedelem, a lopás, a pénzmosás, az uzsorakölcsön, a hitelcsalás és a hitelkártyacsalás. E körben említik még a számítógépes chipek, perifériák és szoftverek ellopását is (uo.).

Napjaink globális biztonsági kihívásai között a legelőkelőbb helyen talán a cyberterrorizmus kérdésköre áll. Tehrani és szerzőtársai 2013-ban Dorothy Denning (2000) alternatív definícióját idézik mint lehetséges, a terrorizmust tágan értelmező megközelítést: „A cyberterrorizmus a terrorizmus és cybertér konvergenciája" (Denning 2000: 1). Ezen általában számítógépek és hálózatok, illetve az azokban tárolt információk ellen elkövetett jogellenes támadásokat és támadásokkal való fenyegetéseket értenek, amelyekkel kormányokat vagy embereket akarnak megfélemlíteni vagy kényszeríteni bizonyos politikai vagy társadalmi célok elérése érdekében. A cyberterrorizmus pedig hatásában éppolyan, mint a „normál" (offline) terrorizmus. Más cyberbűncselekményektől motivációjában és/vagy az elkövetők szándékában tér el. Más megközelítésben a cyberterrorizmus új technológiák használatával elkövetett ugyanolyan típusú erőszak, mint a hagyományos terror (Tehrani et al. 2013).

5 A láthatatlan vagy rejtett web olyan rejtett és/vagy illegális tartalmakkal, amelyeket a standard keresőmotorok nem indexálnak. Szokás *dark web*nek is nevezni. A hagyományos algoritmusok nem biztosítják a(z) (át)láthatóságát.

6 Proaktív politikai szerepvállalás az interneten és/vagy számítástechnikai eszközökön keresztül a szólásszabadság, az emberi jogok és az információ szabadsága jegyében.

7 „Making use of the computer to steal large sum of money."

8 „Theft of services within this definition, as well as invasion of privacy."

9 „Use of a computer to perpetrate any scheme to defraud others of funds, services, and property."

A magyar büntetőjog az informatikai bűncselekmények körébe sorolja az adatvédelmi bűncselekményeket, a szerzői jogot sértő vagy ahhoz kapcsolódó bűncselekményeket, a tiltott pornográf felvétellel való visszaélést, a számítástechnikai bűncselekményeket, s emellett beszél még az előbbi körökbe nem tartozó, számítógéppel érintett (számítógéppel kapcsolatos) bűncselekményekről *(computer-related crimes)* (Szathmáry 2012). Ez utóbbi kategóriába sorolható például az internetes zaklatás, rágalmazás, becsületsértés és más olyan számítógéppel kapcsolatos eset, ahol az elkövetett cselekmény tárgya nem maga a számítógépes rendszer, a tárolt adat, az információ vagy a kommunikációs rendszer. A jelen (és a jövő) egyik legfőbb biztonsági kihívását az interperszonális kapcsolatokon keresztül megvalósuló – számítógéppel kapcsolatos – bűncselekmények bővülő és alig feltérképezett köre jelenti. A virtuális világokba belépő ember sérülékenysége és védelme számos kérdést vet fel, amelyre a rendészeti szakmának záros határidőn belül válaszokat kell találnia. A virtuális és/vagy kevert színterek természetét, jelenségeit és törvényszerűségeit kell a rendészeti szakmának megértenie és mind szemléletébe, mind gyakorlatába beépítenie.

Szathmáry Zoltán (2012) maga is úgy látja, hogy a jog számára problematikus az ember kommunikációs magatartásaival kapcsolatos tényállások definiálása. Főként azért, mert a magánélet fogalma is változóban van, részben épp a megváltozott digitális környezet miatt. A privacy mint az énhez való hozzáférés engedélyezése a közösségi interakciók szabályozásán keresztül valósul meg az online térben menthető, visszakereshető és másolható adatokkal a háttérben. Különösen nehéz a jogalkotó és -alkalmazó dolga az információs társadalomban, mert nemcsak az egyén (annak privát információi, gondolatai, teste, jó hírneve, becsülete és identitása) áll védelem alatt a hozzáférhetőség szempontjából, hanem családja, háztartása és önkéntes választásain nyugvó társas kapcsolatai (beleértve az online közösségeket) is (uo.).

A rendészet dolga e területen a megelőzés volna, de eszközei igen korlátozottak, a már elkövetett bűncselekmény pedig magánindítványra üldözendő, azaz alapja a sértett feljelentése. Szathmáry Zoltán különösen aggályosnak tartja a „veszélyes látszatkeltés" tényállásának bekerülését a törvény szövegébe. E szerint ugyanis bűncselekményt követ el az is, aki egy be nem következő esemény megtörténésének reális esélyét hiteti el a sértettel. Ezt hívjuk a hétköznapi életben színlelésnek, csakhogy a virtuális valóságok alapesszenciája a színlelt, a nem valós, a csak potenciálisan jelen lévő… Ezt tetézi az anonimitás lehetősége: a realitásokat fiktív elemekkel tarkító vagy felülíró avatarokon keresztüli jelenlét. Ács Péter 2014-es tanulmányában arra hívja fel figyelmünket, hogy a számítógépes alkalmazások kommunikációs megközelítésekor a hagyományos individuális és kollektív ágenseken túl számolnunk kell olyan új típusú ágensekkel, mint a voltaképpeni, a fiktív, a mimetikus,[10] a virtuális és az összetett ágensek[11] (Ács 2014).

A megfigyelés és önmegfigyelés kultúrája

A cybertér kihívásaira adott válasz a rendvédelmi szervek részéről csak egyfajta „cyber policing"[12] lehet. Az információs társadalom rendvédelmi kihívásai új képességeket és a rendészeti funkciók kiterjesztését követelik meg. Ez technológiai, instrumentális és normatív kérdések újragondolását is szükségessé teszi.

Fehér Katalin ugyanakkor felhívja a figyelmünket arra, hogy a védelem a felhasználó szempontjából nem feltétlenül és nem elsősorban elzárkózást jelent, sokkal inkább autonómiát és önkontrollt. A felhasználónak szabályoznia kell, hogy privát szféráját kinek és mennyire teszi hozzáférhetővé. Ez egyfajta egyensúlykeresés, ahol a mérleg egyik serpenyőjében a biztonság, az én védelmezésének igénye, a másikban a jövő ígérete és a (személyes adatokért cserébe) megszerezhető előnyök (például ingyenes szolgáltatások) vannak (Fehér 2016).

10 Mimetikus az az A ágens, amely úgy tesz, mintha nem A volna, hanem mondjuk B, s lehet interpretatív annyiban, hogy referálhat egy valahol létező C ágensre (közvetítheti, megjelenítheti annak karakterisztikáját) (lásd még Ács 2014).

11 A kommunikáció participációs elmélete szerint az ágens saját világgal és különféle felkészültségekkel rendelkező aktor, aki vagy amely képes rá, hogy környezetéhez aktívan viszonyuljon (lásd még Horányi 2007).

12 Ezt a terminust egyelőre a szakmai és a közbeszéd sem használja, a rendészet azonban mindinkább a *cyber crime* fogalmának függvényében ad választ arra, mi is a feladata a cybertérben.

Mára mindannyian megfigyelők és megfigyeltek vagyunk. A *dataveillance* (adatmegfigyelés és -felügyelet) korában élünk, ahol kamerarendszerek őrködnek köztereink, tömegközlekedési eszközeink, közútjaink, irodaházaink és magánlakásaink biztonsága felett. Mindezt tudjuk, hiszen kihelyezett táblák, ikonok és egyéb tájékoztatók hívják fel rá a figyelmünket a megfigyelés helyén. Zsörtölődünk az intelligens traffipaxok miatt, de elfelejtjük, hogy a megfigyelés számos más területen is jelen van. A viselkedésünk monitorozása gyakran nem is tudatosul, pedig a közösségi médiában sem teszünk mást, mint figyeljük ismerőseinket, és várjuk, hogy kövessenek minket, lájkolják bejegyzéseinket, kommenteljék közzétett adatainkat, állapotfrissítéseink megjelenjenek hírfolyamukban – és viszont. A szolgáltatók immár egyre differenciáltabb érzelemkifejezőink szerint osztanak minket kategóriákba, hogy a szolgáltatás vagy a termék hipercélzása még pontosabb legyen. (A Facebookon is megjelentek a kedvelés mellett a csodálkozást, a szomorúságot, a dühöt, a hálát kifejező gombok.) A megfigyelés ezzel a mindennapjaink rutinja lett. Magánemberként is részesei vagyunk, s tudjuk, hogy a hatóság is kiaknázza ezeket a felügyeleti csatornákat. Telefonjaink cellainformációi másodpercre pontosan megmondják, merre járunk, lépésszámláló és fitnessalkalmazásaink szokásos útvonalainkat is az elemző elé tárják. Tömeges megfigyelés alanyai lehetünk bármikor, ha a titkosszolgálatok kormányzati felhatalmazással a külső erők ellen úgy kívánnak megvédeni bennünket, állampolgárokat, hogy titkos megfigyelést végeznek (Fehér 2016). „Magyarországon egyetlen ember sincs, akit törvényes körülmények között ne lehetne megfigyelni, lehallgatni" – mondta 2016 májusában Magyarország belügyminisztere, Pintér Sándor a nemzetbiztonsági bizottság ülésén,[13] s e napokban arról cikkez a média, hogy az új büntetőeljárási kódex értelmében már gyanú sem szükséges a titkos információgyűjtés megkezdéséhez.[14]

Ennél összetettebb monitorozást jelent a *surveillance,* a digitális felügyelet azon formája, amely változó információkban (tevékenységek, viselkedések) keres mintázatokat a védelem érdekében (Fehér 2016). Amikor a felhasználó maga is megfigyel, monitorozza a vele történteket, testen viselhető eszközökkel rögzíti az eseményeket, akkor *sousvillance*-ról beszélünk. Erre nyújtanak példát a hordozható (viselhető) kamerává alakítható mobiltelefonok és e célra fejlesztett applikációik, valamint Steve Mann professzor fejlesztései.

A *sousveillance* fogalmát az a Steve Mann professzor használta elsőként, akit az első *cyborg*ként[15] is emlegetnek. Már az 1970-es években testen viselhető eszközök tervezésével foglalkozott, jócskán megelőzve korát, hiszen akkortájt a számítógépek még nagyszobányi helyiségeket foglaltak. Elsőként váltott útlevelet is cyborgként 1995-ben. 1980 óta dolgozik a digitális szem kifejlesztésén. Az ő nevéhez fűződik az első testen viselt kamerával kapcsolatos cyborg fogyasztói incidens is: 2012-ben arról számolt be, hogy bár orvosi papírja volt a fején viselt szerkezet szükségességéről, amellyel szubjektív nézőpontú képeket, felvételeket tudott készíteni, Párizsban mégis kidobták egy McDonald's-ból. Az indoklás szerint a vendégek nem jogosultak felvételt készíteni az étteremben. Mann különböző expozíciós idővel készült felvételeket alkalmazva olyan részletgazdag felvételeket állít elő, amelyek messze meghaladják az emberi szem képességeit. Találmányától pedig azt reméli, hogy idővel, a fejlesztés következő állomásait elérve látássérült vagy memóriazavarral küzdő embereknek nyújt hathatós segítséget a mindennapokban (Meskó 2016).

A *coveillance* egy interakció-fókuszú kiterjesztése mindennek, amely a társas helyzetek dinamikájára helyezi a hangsúlyt: a felek figyelnek és megfigyelnek, s ez percepciók szubjektív és akár jelentősen is eltérő sorát eredményezi. A kamera ugyanis mindenki számára mást és mást mutat, eltérő, versengő percepciókhoz vezet, megannyi értelmezést tesz lehetővé, az eredeti dokumentálási cél így a visszájára is fordulhat. Mindennek ellenpólusa pedig a *counterveillance* (ellenmegfigyelés) (Fehér 2016). Az ellenmegfigyelés lényege a monitorozó, detektáló eszközök beazonosítása, a megfigyelés leleplezése, az átláthatóság biztosítása (ami a hatalommal szembeni kontroll eszköze is lehet). Mindez azt mutatja, hogy a megfigyelésnek, a kontrollnak, s ekként a védelemnek számos – mára hálózatokba rendezett – eszköz áll rendelkezésére, amely az automatizálás és a digitális irányítás révén aktív részvételt, az interakció képességét nyújtja. Így lettek a felügyeleti rendszerek (például riasztások kiadása révén) maguk is szereplői mindennapjainknak (uo.).

13 Népszava.hu: Pintér: bárkit le lehet hallgatni, *Népszava.hu*, 2016. május 31., http://nepszava.hu/cikk/1095630-pinter-barkit-le-lehet-hallgatni (utolsó letöltés: 2017. V. 4.).

14 Fekete Gy. Attila: Már gyanú sem lenne szükséges a lehallgatáshoz, *Magyar Nemzet Online*, 2017. március 17., https://mno.hu/belfold/mar-gyanu-sem-lenne-szukseges-a-lehallgatashoz-2390477 (utolsó letöltés: 2017. V. 4.).

15 A *cybernetic organism* rövidítéséből: olyan személy, aki organikus és mechanikus alkatrészeket, azaz bioanyagokat és bioelektronikát használ (Meskó 2016).

Kevert valóságok, metaverzumok

Ha önmagában a virtuális szó jelentését vesszük alapul, igen szabadon, talán túlontúl önkényesen is dönthetjük el, mit tekintsünk virtuális valóságnak: lehet az tényleges, nem valós, látszólagos, lappangó vagy lehetséges. Célszerű ezért a rendészeti szakma számára néhány olyan definíciót keresni, amelyek összecsengő tartalmai utat mutatnak a Facebook, a Twitter, az Instagram, a Pinterest lázában égő, metaverzumokba lépő és virtuális gazdaságot működtető civilekhez.

György Péter megközelítésében a virtuális valóság nem más, mint a retinánkra vetített kép, amelyet digitális technológiával hozunk létre, s beletartoznak a képet létrehozó programelemek és az általa keltett perceptuális élmények is (György 1995).

Az Európai Hálózat- és Információbiztonsági Ügynökség a háromdimenziós virtuális környezeteket olyan jegyeik alapján definiálja, mint a perzisztencia, a központi adatbázisra alapozottság, a valós idejű interakciók, a világok saját(os) működési szabályai, a felhasználók avatarokon keresztüli részvétele (Warren & Palmer 2010). E jegyek egy közös jelentések által konstruált valóságra utalnak,[16] amelyben az ágensek bizonyos normák szerint bonyolítják le interakcióikat. Avataruk egyfajta (akár fiktív elemeket is vagy szinte kizárólag azokat) tartalmazó homlokzat.[17] A technológia oldaláról mindez kiegészül a szinkronicitással, a valóság tartós (a résztvevők jelenlététől független) létével, illetve egy harmadik fél által üzemeltetett és felügyelt adatbázissal.

A pszichológusok és a viselkedéskutatók szempontjából azonban a VR *(virtual reality)* egy olyan új technológia (illetve technológiák sora), amely megváltoztatja az ember–gép-interakciókat. Jellemzője, hogy a felhasználó azt hiszi, egy számítógép által generált 3D-s világban van. Ennek általában feltétele egy fejre illeszthető kijelző *(head mounted display)* vagy más immerzív eszköz, amely biztosítja, hogy a felhasználó belemerüljön az érzékletekbe (Riva et al. 2004). E megközelítésben a VR kulcsfogalmai a belemerülés *(immersion)*, a navigáció és az interakció.

A megnevezések ugyancsak sokfélék. Fehér Katalin ezredforduló előtt végzett kutatásában a képzetes világ, a mesterséges valóság vagy ellenvilág terminusokat sorolja fel mint a sajtóban és a közbeszédben megjelenő kifejezéseket a virtuális tér megjelölésére. Említi még a *cyber space* (kibertér) megjelölést, amely háromdimenziós konszenzuális helyként határozható meg, de általában szűkebb értelemben használja a számítógépes szakma (Fehér 1999).

Az AR, a kiterjesztett valóság *(augmented realitiy)* annyiban tér el a VR-től, hogy nem alternatív (helyettesítő, fiktív karakterisztikájú vagy szimulált, „mintha") világot nyújt a valós helyett, hanem a valós világot bővíti ki virtuális elemekkel. A kiterjesztés valós időben történik, összhangban a valós fizikai tér elemeinek szemantikai kontextusával. Az olyan hozzáadott információkkal, mint egy számítógépes látványelem vagy a tárgyfelismerés, interaktív digitális manipulációk hajthatók végre a felhasználót körülvevő való világ körülményeiben (uo.). A virtuális és a kiterjesztett valóságok alapvető különbsége, hogy míg az előbbi szeparálja a felhasználót a valós világtól, az utóbbi a két világ információinak és tapasztalatainak vegyítését (egyidejű megtapasztalását) valósítja meg (Balkányi & Orbán 2011). A mobilizáció pedig természetszerűleg elhozta a MAR-t *(mobile augmented reality)*, az AR minden okostelefon-használó számára elérhető, hordozható verzióját.

Az első ismert immerzív multiszenzoros technológia, a Sensorama az első cyberbűncselekményekkel egy időben, az 1950-es években született meg. Megalkotója Morton Heilig volt (Matuszka 2012). Az AR és a VR hozta biztonsági kihívások mégis csupán napjainkban kerülnek igazán a média és a tudomány, s ezzel a hatóság figyelemének középpontjába.

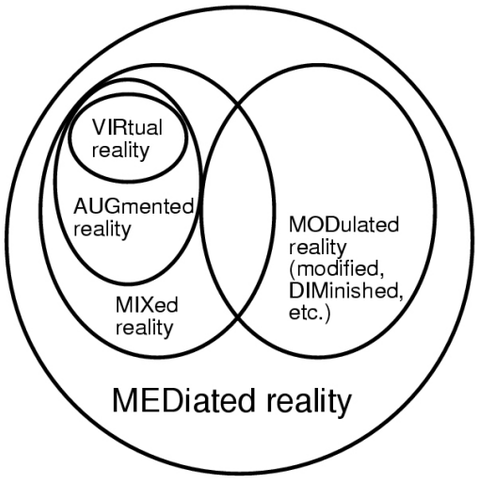
Steve Mann több, mint tíz évvel ezelőtt felhívta a figyelmet arra, hogy mindennapjainkat mindinkább közvetített és kevert valóságokban éljük. A közvetített *(mediated)* valóságok két főcsoportját a, módosított vagy csökkentett *(modulated)* valóságok és a kevert *(mixed)* valóságok alkotják (Mann 2002). A kevert valóságok jellemzője, hogy nem feltétlenül és egészében virtuálisak, de virtuális technológiához kötődnek.[18] Az utóbbi csoportban kell vizsgálnunk a virtuális és a kiterjesztetett valóságokat.

16 Akár a kommunikáció neodurkheimi megközelítése, amely azt mondja, hogy a kommunikációban részt vevő felek közösen adnak jelentést a világ dolgainak, jelenségeinek, így konstruálva a világot és teremtve meg identitásukat. A közösen osztott társadalmi objektivációkon keresztül az egyének interiorizálják a társadalom rendjét, és egyúttal objektiválják magukat, meghaladva személyes identitásukat a közösség tagjává válnak (a részesedés megélése által).

17 Ennek dinamikus oldalaként és a normákkal összefüggésben értelmezhető a szerep fogalma is, amelyet az ágens interakciói során megtestesít.

18 David, Grover (2013): A survey of Mixed Reality, with an emphasis on Augmented Reality. Macquarie University, Sidney, Australia, https://wiki.mq.edu.au/display/ar/AR+background+history+and+terminology, (utolsó letöltés: 2016. V. 31.)

1. ábra
Steve Mann modellje a közvetített valóságok alkategóriáiról



Forrás: Mann (2002)[19]

VR a rendészetben

A VR rendészeti felhasználásában döntő jelentőségűek a virtuális tréningek, szimulációk és az olyan hordozható immerzív terek, amelyek már a tudatalatti információkat is megkísérlik monitorozni és felhasználni az alapvető tudásformák feltérképezéséhez. Részben már a jelen gyakorlatai ezek, részben a jövő továbblépési lehetőségei.

A virtuális tréningek mint az újoncok kiképzésének modern és biztonságos eszközei a rendészeti oktatás új lehetőségeit nyitották meg. Megjelentek az azonnali rendőri és katonai döntéshozatal fejlesztését segítő beltéri, egyes szám első személyű tapasztalást biztosító *(immersive)* szimulációk. Ezek segítségével elsősorban a lőfegyverhasználatot és a fizikai erő alkalmazását gyakorolhatják a rendőrök, beleértve a gyors helyzetfelismerést és döntéshozatalt, a pontos célzást, a megfelelő mértékű erő alkalmazását stb.[20]

Az eredetileg katonai célokra kifejlesztett amerikai VIRTSIM-nek 2012-ben készült el egy új verziója a bűnüldöző szervek igényeire szabva. Bár a polgári rendvédelmi képzésekhez korábban is rendelkezésre álltak szimulációk, a VIRTSIM az egyike a legrealisztikusabbaknak.[21] Elsősorban katonai és veszélyhelyzeti szimulációkhoz biztosít élethű környezetet, amelyben a felhasználók teljes testkövetése valósul meg. Az avatarok képességei igazodnak a felhasználók testalkatához (magasság, testtömeg stb.), és az elszenvedett sérülések valós fájdalommal járnak. A rendőrök tricepszéhez olyan izomstimulátorok csatlakoznak, amelyek – ha találat éri őket a virtuális tűzharc során – áramütéssel idézik elő a fájdalmat. A VIRTSIM előregyártott forgatókönyveket tartalmaz beltéri szimulációkhoz, amelyeket azonban a rendőrségek maguk is új szcenáriókkal egészíthetnek ki.

A technológiai továbblépést pedig már a hordozható immerzív interaktív terek jelentik. Az Európai Bizottság 2012-ben indult CEEDS Projektje integrált és interaktív rendszerek, virtuális terek fejlesztését tűzte ki célul, az emberi

19 Steve Mann: Mediated Reality with implementations for everyday life, *Wearcam.org,* 2002. augusztus 6., http://wearcam.org/presenceconnect/viraugmixmodmediated_reality.png (utolsó letöltés: 2017. V. 22.).

20 VirTra: VirTra Simulator Training Systems, *Virtra.com,* 2017., http://www.virtra.com/useofforcesimulators/ (utolsó letöltés : 2017. V. 13.).

21 Ben Lang: VIRTSIM is the Virtual Reality Platform That Gamert Crave but Cant't Have, *Road to VR,* 2012. november 4., http://www.roadtovr.com/virtsim-virtual-reality-platform/ (utolsó letöltés: 2016. V. 21.).

információfeldolgozás folyamatainak jobb megértése érdekében.[22] Elsőként szintetikus terek létrehozása a cél, amelyekben a felhasználók tudatos tapasztalatairól gyűjtenek adatokat és szűrnek ki mintázatokat, majd megpróbálják kiaknázni a tudatalattiban rejlő lehetőségeket például a meglepetések, a felfedezések tudatalatti folyamatainak monitorozása révén. Ezzel a tudás alapvető formáit próbálják felszínre hozni a virtuális terekben agy–gép-interfészek adatainak rögzítésével és elemzésével. A technológia alapját testen viselhető vezeték nélküli érzékelők (például vezeték nélküli biofeedback ing) és 3D-s kamerák jelentik. A Budapesti Műszaki Egyetem által fejlesztett CEEDs pXIM2.0 rendszer alkalmazási területei között szerepel az agyi területek közötti összefüggések vizualizációja, a kollektív érzelmi élmények rögzítése.[23]

A virtuális fenyegetettségekre adott válasz a rendvédelmi szervek részéről egyelőre még inkább csak a közösségi médiajelenlétet jelenti: a Facebook-profilokat, Twitter-hírfolyamokat, a Skype-ügyeletet (Egyesült Királyság) és jobb esetben a virtuális rendőrőrsöket (India, Delhi). 2015 óta a különféle felügyeleti kamerarendszerek telepítése vett nagy lendületet (különösen az Egyesült Államokban, de a világ más táján is), illetve a virtuális járőrözés különféle formái. Ez utóbbit máig nem sikerült úgy megvalósítani, hogy az állampolgárok számára látható és elérhető formában legyen jelen, annak ellenére, hogy Kínában 2007-ben tűnt fel például az első virtuális járőr az online térben.[24]

2. ábra
Az első pekingi virtuális járőrök

Forrás: China Daily, 2007. augusztus 29.

Etikai aggályok a VR rendvédelmi és katonai célú felhasználásával kapcsolatban

A VR-ről a pszichológia a technológiai megközelítésektől eltérően gondolkodik: „A pszichológia a virtuális realitás fizikája" (idézi Biocca 2003). William Bricken 1990-ben e mondatával kívánta felhívni kortársai figyelmét arra, hogy a VR megértésében, természetének feltárásában sokkal nagyobb figyelmet kell(ene) fordítani a VR elmére gyakorolt hatására, mint a fizikai törvényszerűségek leképezésére vagy felülírására. A kiterjesztett térrel és mérnöki kihívásaival szemben inkább a *kiterjesztett elméről* kell gondolkodnunk, amely Bricken értelmezésében az a hely, ahol a tapasztalás, a technológia és a pszichológia találkozik (uo.).

2016 márciusában számolt be arról a mainzi Johannes Gutenberg Egyetem, hogy kutatói, Michael Madary és Thomas Metzinger kidolgozták az első etikai (magatartási) kódexet a virtuális világok üzemeltetői számára.[25] Aggályukat fogalmazták meg a virtuális valóságok olyan tulajdonságainak tekintetében, mint hogy

- a felhasználó megéli egy olyan test birtoklásának és kontrollálásának érzetét, amely nem is az övé,
- a virtuális tér elhagyása után is fennmaradó viselkedési hatások érik a felhasználókat,

22 CEEDs. The Collective Experience of Empathic Data Systems: About CEEDs, 2017, https://ceeds-project.eu/ceeds-objectives/aboutceeds/ (utolsó letöltés: 2017. V. 21.).

23 BME: Hordozható immerzív interaktív tér magyar fejlesztésben, *BME,* 2012. október 19., https://www.bme.hu/k%2Bf%2Bi/20121019/immerz_interaktiv_ter (utolsó letöltés: 2016. IV. 29.).

24 Xinhua: Virtual Beijing police to patrol in cyber world, *China Daily,* 2007. augusztus 29., http://www.chinadaily.com.cn/china/2007-08/29/content_6066310.htm (utolsó letöltés: 2016. VI. 01).

25 Johannes Gutenberg-Universität Mainz: First code of conduct for the use of virtual reality established, 2016. március 4., https://www.uni-mainz.de/presse/20156_ENG_HTML.php (utolsó letöltés: 2016. IV. 21.).

- fennáll a szándékos (tudat alatti) manipuláció lehetősége a virtuális terek megalkotói részéről (vallási, politikai, kereskedelmi, kormányzati vagy egyéb érdektől vezérelve),
- a felhasználókat olyan erős hatások ér(het)ik, amelyek hosszú távon is hatással vannak/lehetnek énképükre, önértékelésükre.

Madary és Metzinger érvei között szerepel a kontextus-érzékenység *(context-sensitivity),*[26] amely akár eddig ismeretlen epigenetikus tulajdonság kialakulásához is vezethet az új környezetben; az illúziók megélésének intenzitása – egészen a társas hallucinációkig bezárólag –, s azok tartós hatása (a kiváltott és mélyen megélt érzelmek által); valamint a felhasználói identitás közvetlen manipulációja (például a valóssal nem egyező testkép, képességek, tulajdonságok révén) (Madary & Metzinger 2016).

3. ábra
Kínzás VR technológiával?

Forrás: Rodger 2013[27]

A kutatók bebizonyították, hogy a VR felhasználásával képesek empátiát kiváltani két idegen között, de ezzel együtt felismerték a VR „sötét oldalát" is: ugyanilyen könnyedén okozható fájdalom, szenvedés mind fizikai, mind érzelmi síkon, és ezzel létrejött a pszichológiai kínzás új eszköze.[28]

Mindez felveti a virtuális világok katonai és rendészeti felhasználása esetén a szándékos pszichológiai és fizikai kényszerek, akár a kínzás, a kínvallatás alkalmazásának lehetőségét. Hiszen a fejlett avatartechnológia[29] révén gyorsan és rugalmasan lehet változtatni a környezetet és a szabályokat a viselkedés befolyásolásának célzatával.

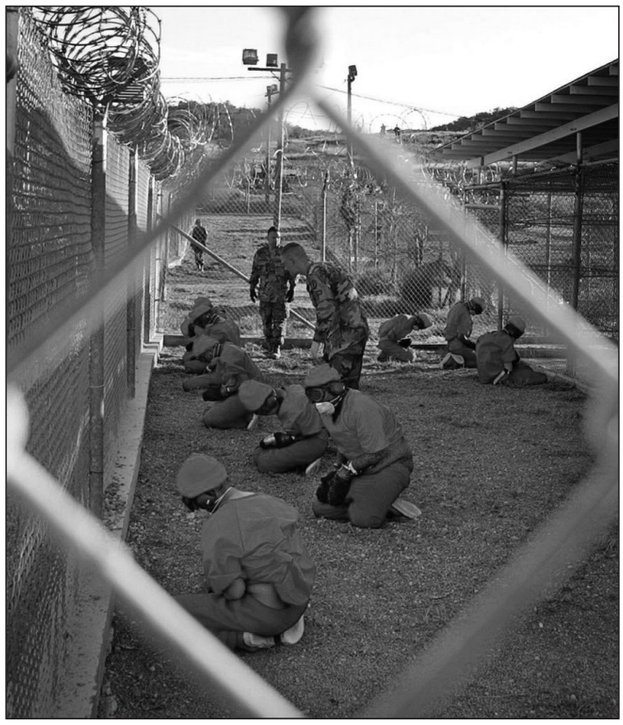
26 Az ágens (és az intelligens rendszerek) azon tulajdonsága, hogy a környezeti információkra reagál, viselkedését az észlelt kontextuális tér viszonyaihoz igazítja. Feltétele a kontextuális érzékelés *(contextual sensing)*.

27 David J. Rodger (2013): Twitter Feedback about Yellow Dawn – The Age of Hastur (RPG) and Dark Sci-fi Novels, *WordPress.com,* 2013. december 10., dark-science-fiction-immersive-virtual-reality-junkie, davidjrodger.wordpress.com, https://davidjrodger.files.wordpress.com/2013/12/dark-science-fiction-immersive-virtual-reality-junkie-image-source-unknown.jpg (utolsó letöltés: 2017. V. 23.).

28 Jason Johnson: We should be talking about torture in VR, *Killscreen.com,* 2017. április 25., https://versions.killscreen.com/we-should-be-talking-about-torture-in-vr/ (utolsó letöltés: 2016. V. 13.).

29 Avatartechnológia: olyan szoftverfejlesztői megoldások, amelyek a felhasználó számára lehetővé teszik személyes (digitális/virtuális) reprezentációja létrehozását akár egy weboldalon vagy más kommunikációs csatornán keresztül (tetszőleges digitális/online színtéren), módot adva érzelmei, gondolatai ki kifejezésére, másokkal való együttműködésre stb. Ehhez szükség lehet valamilyen asztali alkalmazásra, speciális szoftver telepítésére vagy online elérésére. A mögöttes technológiák a fejlesztők szerint közhelyesek (TCP / IP csomagok, UDP, FTP, http vagy egy „valamilyen" plug-in). (Mason 1999)

4. ábra
Guantanamói fogvatartottak érzékszervi megfosztása (2002)



Forrás: i1.wp.com (2016)[30]

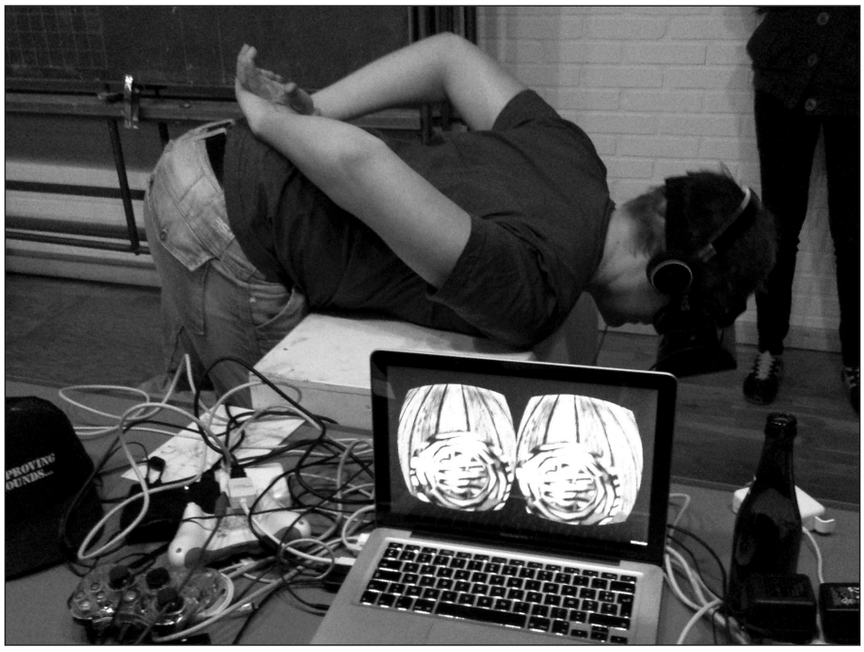
A VR-ben külsérelmi nyom nélkül vihető véghez az erőszak, a bántalmazás számos formája, amelyet így nehéz, hacsak nem lehetetlen bizonyítani (és épp ezért megelőzni vagy felderíteni s szankcionálni is). Egyetlen fejre illeszthető kijelző képes zavartságot, valamilyen betegség érzetét vagy pánikot előidézni, félelmet kelteni, vallási vagy erkölcsi becsületsértést, szenzoros túlterhelést vagy épp deprivációt kiváltani, egy érzék (vagy testrész) elvesztésének érzetét kelteni, függőséget okozni (uo.).

A VR-ben való hosszas elmerülés ráadásul megváltoztatja a személy reagálását a vizuális ingerekre, önmaga érzékelését, valamint idő- és térérzékelését is.[31] Mindez hallucinációkhoz vezethet, ami kiválthatja a fogvatartottak önpusztító magatartását is. Játszi könnyedséggel hozhatók létre fantomérzések *(body transfer illusion)*. A szakértők egyetértenek abban, hogy a szimulált kínzás éppen olyan hatékony, mint az igazi. Ha valaki úgy gondolja, kínozzák, akkor kínozzák. Hiszen a valóság nem más, mint amit a valóságból észlelünk (Bierend 2015).

30 Lásd: https://i1.wp.com/versions.killscreen.com/wp-content/uploads/sites/2/2016/03/Camp_x-ray_detainees.jpg?w=684&ssl=1 (utolsó letöltés: 2016. V. 21.).

31 Az egyik aggály, amelyet a kutatók megfogalmaztak a virtuális valóságokkal kapcsolatban, az a kinetózis vagy utazási betegség *(VR sickness)*, amely éppen abból adódik, hogy a valós és a virtuális körülmények együttes jelenléte kognitív disszonanciához vezet. Merthogy a virtuális világban tett akcióink közben testünk rendszerint nyugalomban van, agyunk azonban a szimulált érzékletek fogságában aktivizálódik.

5. ábra
Guillotine-szimulátor (Berlemont, Brunbjerg, Trummal)



Forrás: Berlemon (2013)[32]

Csak példaként említjük meg Andre Berlemont, Morten Brunbjerg és Erkki Trummal guillotine-szimulátorát, amely a felhasználó számára azt az „élményt" nyújtja, mintha nyaktiló pengéje sújtana le a nyakára, miközben barátja ütést mér rá, s azután láthatja a megfelelő perspektívából saját fejét elgurulni vagy kosárba esni (LaValle 2016).

Michael Madari és Thomas K. Metzinger épp a fentiek okán látta szükségesnek megfogalmazni a legfőbb etikai ajánlásokat a VR használatával kapcsolatban. Összhangban az Amerikai Pszichológiai Társaság elveivel, biztosítani kell, hogy a virtuális valóságok ne okozhassanak maradandó vagy súlyos károsodásokat. A VR-be belépőket tájékoztatni kell a komoly és (esetleg) tartós viselkedési hatásokról és arról, hogy azok mértéke és hatása nem ismert (nem jelezhető előre). A kutatóknak és a médiumoknak kerülniük kell a virtuális világok túlzó bemutatását, (agresszív, intenzív) népszerűsítését, különösen, ha az mint orvosi kezelés (terápiás eszköz) kerül tárgyalásra. A felelős adatkezelés és a személyiségi jogok védelme még szigorúbb kívánalomként jelentkezik, hiszen a felhasználói adatok eddig nem látott köre kerül monitorozásra a rendszerekben. Nemcsak a tudatos, hanem a tudat alatti válaszok, apró szemmozgások, mimikai és egyéb nonverbális jelzések, fiziológiai reakciók (szívverés, testhőmérséklet stb.) is rögzíthetők.

Testen viselhető és beültethető eszközök

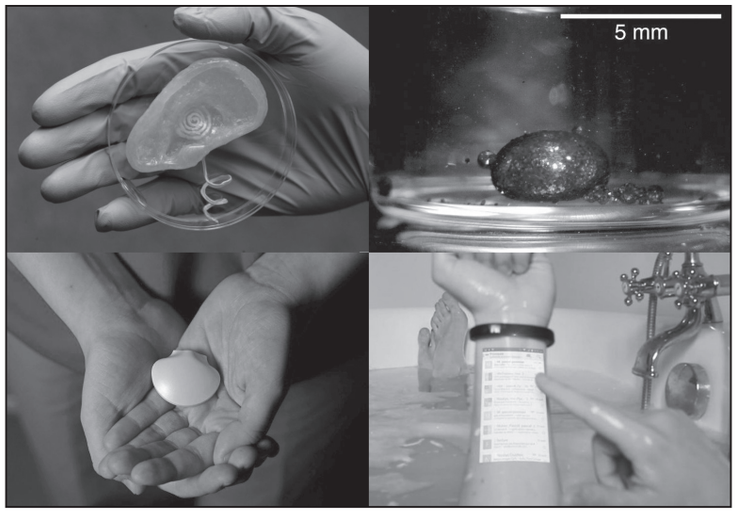
Ma már léteznek olyan alkalmazások is, amelyek túlmutatnak a mobiltechnológián. Csak az első lépést jelentik azok a szoftverek, amelyek a telefont testen viselhető videokamerává változtatják, automatikusan dátum, idő és hely (GPS-adat) címkével látják el a felvételeket (Video Armor: Police Camera).[33] Ugyanakkor ezek az alkalmazások arra irányítják a figyelmet,

32 André Berlemon: Disunion - The guillotine simulator, *Vimeo.com,* 2015. május 5., https://vimeo.com/65510054, (utolsó letöltés: 2016. V. 21.).

33 Police One (2016): Police Android Apps, *PoliceOne.com,* http://www.policeone.com/police-android-apps/, (2016. VI. 03.).

hogy nem pusztán mobil, hanem mindinkább testre szabott és a testen viselhető *(wearable)* és az implantálható *(implantable devices)* megoldások felé mozdulnak a fejlesztések. A várakozások az implantálható (beültethető) okostelefonokat említik elsőként. Tavaly ugyanis Anthony Antonellis már beágyazott egy RFID chipet a karjába, hogy az adatokat tároljon és továbbítson okostelefonjára. A tudósok pedig ez idő szerint azzal kísérleteznek, hogy az emberi csontok használhatók-e élő hangszórókként a testbe ültetett eszközök számára. Ennek mintájára kísérleteznek azzal is, miként rögzíthet a szem képeket egy adattároló számára, és az hogyan volna megjeleníthető a bőrön mint kijelzőn keresztül.[34]

6. ábra
A jövő implantálható eszközei
(okos szerv, okos por, gyógyító chip, okostelefon kijelzője a csukló bőrén)



Forrás: WT VOX

A fejlesztések célkeresztjében állnak továbbá különféle orvosi monitoringeszközök (keringés-, vércukor-, vérzsírmérők és -szabályozók), gyógyító chipek *(healing chip)*, adattovábbító tabletták vagy irányított (például fogamzásgátló) cyberkapszulák *(cyber capsule, cyber pills)*. Azután jöhetnek az okostetoválások *(smart tattoo)*, a nanotechnológia segítségével előállított okospor *(smart dust)*, az agy–számítógép-interfészek *(brain-computer interface)*, a biológiailag lebomló elemek *(biodegradable bio-batteries)* és a beültethető 3D-s okos szervek, az én azonosítására és felügyeletére kidolgozott eszközök *(verified self)* (uo.).

A szakértők ugyanakkor arra is felhívják a figyelmet, hogy az új – elsősorban gyógyászati – technológiák a bioterrorizmust is új szintre emelik. Az egyik legnagyobb kockázatot az rejti, ha a bennünk lévő eszközökhöz (például nanorobotokhoz) kívülről férnek hozzá illetéktelenek (Meskó 2016). Gondoljunk bele, milyen támadások hajthatók végre, ha szívritmus-szabályozót lehet meghekkelni, nanorobotot távvezérelni és bioanyagokat szabotálni!

Ezek a technológiák már az ember–gép-határ elmosódását hozzák magukkal, a *transzhumán létezés* alapjait rakják le. Mindez már a „jelenlévő jövő"[35] (Fehér 2016).

34 Medix (2015): Top 10 Implantable Wearables Soon To Be In Your Body, *WT VOX,* 27th October 2015. október 17., https://wtvox.com/3d-printing/top-10-implantable-wearables-soon-body/, (2016. VI. 13.)

35 Olyannyira így van ez, hogy 2016 őszén rendezték meg Zürichben az első cybathlont, azon paraatlétáka sportversenyét, akik high-tech protéziseket, külső motoros csontvázakat és más robotokat vagy kiegészítő eszközöket használnak a sportversenyen. Elgondolkodtató a tény, hogy a parasport ezen új ágában az egyik legnagyobb várakozással tekintett sportág az agy–számítógép-interfészek (és persze a fejlesztők) versenye (http://www.cybathlon.ethz.ch/).

Összefoglalás

E tanulmány a digitális technológiák és a megváltozott kommunikációs színterek, mediatizált valóságok hozta változásokra reflektál. Merít a kognitív tudományok, a pszichológia, a kommunikáció- és médiatudomány, a rendészettudomány, a jogtudomány és az informatika diszciplináris eredményeiből is. Középpontjában mindvégig az ember és a számítógép kapcsolata, s a mára részben megvalósulni látszó transzhumán lét áll.

A kiberbűncselekmények rövid történeti felvezetését követően szó esik az adatfelügyeletről, a megfigyelés kultúrájáról, amely mára mindannyiunk (gyakorta észrevétlen) mindennapi rutinjává vált. Ezt követően bemutatásra kerültek a virtuális és a kiterjesztett valóságok, azok immerzív jellege, a felhasználók számára kihívást jelentő szenzoros sajátosságok. A tanulmány igyekezett számba venni a virtuális valóságokkal kapcsolatos etikai és rendészeti aggályokat, rámutatva, hogy a mérnöki megoldásokkal szemben nagyobb figyelmet érdemelnek az elme (a kiterjesztett elme), valamint az agy és a test interakciójának kérdései. Madary és Metzinger nyomán bemutatta az elsőként megszületett etikai ajánlásokat, amelyek a VR-hype kockázatainak csökkentésére születtek. Zárásként felvillantotta a jövő néhány ígéretes okoseszközét (okospor, kiberkapszula, okostetoválások stb.), amelyek fejlesztése még éppen csak elindult. A tanulmány ekként jelzés és figyelemfelhívás kíván lenni, hogy a rendészetnek a digitális ágazatokban erősödnie kell.

Felhasznált irodalom

Ács Péter (2014): Kommunikációs eszközök és a virtuális ágens. Számítógépes alkalmazások kommunikációs megközelítése. In: Demeter Márton (szerk.): *Konstruált világok. A jelenségek kommunikatív leírása*, 108–128. o. Budapest: Typotex.

Balkányi Péter & Orbán Zsolt (2011): Virtuális információk a fizikai térben: a kiterjesztett valóság jövőképe. *Információs Társadalom*, 11. évf., 1–4. sz., 64–80. o., http://epa.oszk.hu/01900/01963/00035/pdf/EPA01963_informacios_tarsadalom_2011_1_4_064-080.pdf (utolsó letöltés: 2016. V. 30.).

Bierend, Doug (2015): The Dark Age of Virtual Reality-Based Torture Is Approaching Fast, *Motherboard,* január 31., http://motherboard.vice.com/read/how-virtual-reality-could-be-used-for-torture (utolsó letöltés: 2016. VI. 13.).

Biocca, Franc (2003): Preface. In: Giuseppe Riva & Fabrozio Davide & Wijnand Ijsselsteijn (eds.): *Being There. Concepts, effects and measurements of user presence in synthetic environments*, *Emerging Communication,* vol. 5., http://www.emergingcommunication.com/volume5.html (utolsó letöltés: 2016. VI. 02.).

Cortada, James W. (2008): *The Digital Hand. How Computers Change the Work of American Public Sector Industries*, vol. 3. New York: Oxford University Press.

Denning, Dorothy E. (2000): Cyberterrorism: The Logic Bomb versus the Truck Bomb. *Global Dailogue. Terrorism: Image and Reality*, vol. 2, no. 4, http://www.worlddialogue.org/content.php?id=111 (utolsó letöltés: 2016. VI. 22.).

Fehér Katalin (2016): *Digitalizáció és új média. Trendek, stratégiák, illusztrációk*. Budapest: Akadémiai Kiadó.

Fehér Katalin (1999): Metafórák a virtuális valóság jellemzésére a magyar sajtóban. *Jel-Kép*, 4. sz., 49–62. o., http://www.c3.hu/~jelkep/JK994/feher/feher.htm (utolsó letöltés: 2016. V. 22.).

György Péter (1995): Szép új világkép. *Filmvilág*, 3. sz., 38–41. o., http://www.filmvilag.hu/xista_frame.php?cikk_id=731 (utolsó letöltés: 2016. IV. 03.).

LaValle, Steven M. (2015/2016): *Virtual Relaity*, University of Illinois, (draft) Copyright Steven M. LaValle, http://vr.cs.uiuc.edu/ (utolsó letöltés: 2016. V. 30.).

Mason, Moya K. (1999): *Avatar Technology*, http://www.moyak.com/papers/avatars-damer.html (utolsó letöltés: 2017. V. 22.).

Madary, Michael & Thomas K. Metzinger (2016): Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology, *Frontiers and Robotic in AI,* 2016. február 19., http://journal.frontiersin.org/article/10.3389/frobt.2016.00003/full (utolsó letöltés: 2016. VI. 22.).

Mann, Steve : Mediated Reality with implementations for everyday life, *Presence Connect,* 2002. augusztus 6., http://wearcam.org/presence-connect/, (utolsó letöltés: 2016. VI. 22.).

Matuszka Tamás (2012): *Kiterjesztett valóság alkalmazások fejlesztése, elemzése és a fejlesztőeszközök összehasonlítása*. Diplomamunka. Budapest: Eötvös Loránd Tudományegyetem Informatikai Kar, Média- és Oktatásinformatika Tanszék.

Riva, Giuseppe & C. Botella & P. Légeron & G. Optale eds. (2004): C*ybertherapy: Internet and Virtual Reality as Assessment and Rehabilitation Tools for Clinical Psychology and Neuroscience*, Amsterdam: IOS Press, http://www.cybertherapy.info/pages/book3.htm (utolsó letöltés: 2016. VI. 2.).

Szathmáry Zoltán (2012): *Bűnözés az információs társadalomban. Alkotmányos büntetőjogi dilemmák az információs társadalomban*. PhD értekezés, Budapest: PTE ÁJK 2012. elektronikusan: http://ajk.pte.hu/files/file/doktori-iskola/szathmary-zoltan/szathmary-zoltan-vedes-ertekezes.pdf (utolsó letöltés: 2016. III. 21.).

Tehrani, Pardis Moshlemzadeh & Nazura Abdul Manap & Hossein Taji (2013): Cyber Terrorism Challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law and Security Review,* no. 29, pp. 207–215.

Warren, Ian & Darren Palmer (2010): Crime risks of three-dimensional virtual environments. *Trends & Issues in Crime and Criminal Justice,* February 2010, no. 388, http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi388.pdf (utolsó letöltés: 2016. VI. 22.).

Wu, Jennifer (2013): Choosing My Avatar & the Psychology of Virtual Worlds: What Matters?, *Kaleidoscope,* vol. 11, article 89, http://uknowledge.uky.edu/kaleidoscope/vol11/iss1/89 (utolsó letöltés: 2016. VI. 1.).

Abstract

This study will navigate the readers into the word of virtual and augmented realities. It aims to highlight some new challenges and ways of misuse that many professions from communications to law enforcement have to reconsider in the digital era. The main question is, what happens when we step into the VR, what new dimensions of our vulnerability open up, what kind of phenomena have to be discussed in multidisciplinary approaches. The nature of cyber crime has changed and so has its scene, the phenomenon of privacy is always changing as we all change ourselves and transform the cultural environment. Our lives are more and more intertwined by technology, mediated realities and surveillance. Only one step is the transhuman being, so it is time to take a look at the direction we are heading to.

Kriskó Edina PhD, kommunikációs szakember, tréner, mediátor. A Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Karának adjunktusa. A Szegedi Egyetem Bölcsészettudományi Karán diplomázott public relations és nemzetközi kommunikáció szakirányon, majd a Pécsi Tudományegyetem Nyelvtudományi Doktori Iskolájának Kommunikáció programjában védte meg a magyar rendőrség sajtókommunikációjáról szóló doktori értekezését (2013). Oktatási tapasztalatot a Gábor Dénes Főiskolán (2006–2009), a Budapesti Gazdasági Főiskola Külkereskedelmi Karán (2010–2014), illetve a Közszolgálati Egyetemen (2012–), valamint jogelődjénél, a Budapesti Corvinus Egyetem Közigazgatás-tudományi Karán (2011) szerzett. Rendszeresen tart vezetői és készségfejlesztő tréningeket, workshopokat. Kutatásait a szervezeti kommunikáció, a második generációs webalkalmazások *(social media),* illetve a kríziskommunikáció területén végzi.