NEMESLAKI ANDRÁS

A REPLIKA ÉS AZ INFORMÁCIÓS TÁRSADALOM CÍMŰ FOLYÓIRATOK KÖZÖS SZÁMA

A Replika és az Információs Társadalom folyóiratok szerkesztői rendkívül innovatív és ötletes kezdeményezéssel álltak elő 2017/3 és 2017 1. számukkal, amelyekben azonos témakörben, egymásra hivatkozva és összekapcsolva jelentettek meg 9 tanulmányt és 2 konferencia beszámolót. A magyar társadalomtudományban két okból is eredeti és komoly hatású ez az ötlet; egyrészt azért mert az olvasó közönség illetve elérhetőség ily módon sokkal tágabb lehet az egyébként sajnos szűkös hazai szakmai érdeklődők körében, másrészt az adott témakör feldolgozási mélysége is sokkal alaposabb, többoldalú, módszertani szempontból is szerteágazóbb lehet. Ez a témakör az információs társadalom egyik jelenleg legizgalmasabb – sokak szerint legellentmondásosabb – kihívása, amit átfogóan kiberbiztonságnak nevezhetünk; azon belül is három kérdéskör, az első a korszerű IKT eszközök hatása a magánszféra és a biztonság viszonyára, a második az adataink védelmével és az azokat érő támadások sajátosságával, végül a harmadik a mesterséges intelligenciával körülölelt világunkban az algoritmusok hatásaival foglalkozik.

Recenziómban a cikkeket, illetve a tárgyalt témaköröket nem a megjelenésük sorrendjében mutatom be, hanem egy olyan értelmezésben, amely szerintem a technika-tudomány-társadalom (science-technology-studies) program egyik legújabb irányának megfelelő. Az STS kutatások ugyanis azt vizsgálják, hogyan konstruálunk „dolgokat" (Sismondo, 2008) egy folyamatosan bővülő vizsgálati tárgyú, multidiszciplináris közelítés- és szemléletmódban. Tudományos ismeretekből kiindulva fokozatosan terjedt ki a technikai műtárgyak, anyagok, intézmények, jelenségek, történetek és kultúrák területére (Hackett, Amsterdamska, Lynch, & Wajcman, 2008). Átolvasva a Replika és Információs Társadalom magánszférával és biztonsággal foglalkozó cikkeit, számomra egyértelműnek látszik, hogy nemcsak tankönyvértékű összefoglalásokról van szó, hanem az STS program nemzetközi szinten is értékes továbbfejlesztéséről.

A téma alapfelütését Charles D. Raab cikkének fordítása adja meg, amelyik „A magánszféra, mint biztonsági érték" címet viseli. A magánszféra kérdéseit, azaz, hogy az egyén hogyan viszonyul az őt érő támadásokhoz, ellenőrzéshez, esetleg szabadságának korlátozásához, számos esetben gondolták újra a jog és társadalomtudomány különböző területein. Raab pl. említi a 2001. szeptember 11-ét, ami után a világ nagyot változott a magánszféra prioritása – a „békén hagyás jogosultsága (the right to be left alone)" – a társadalmilag ugyancsak komoly értékkel bíró biztonság prioritásával szemben. Azóta is számos terrortámadás történt a világ több pontján, amelyek folyamatosan napirenden tartják a demokratikus államok egyik legnagyobb újkori kihívását; azt hogy létezik-e alku a személyiségi jogokat érintő magánszféra feladása, illetve az állam gondoskodó beavatkozása között a nagyobb társadalmi biztonság megteremtése érdekében. Az USA-ban az NSA felállítása egyértelműen nemzeti érdekekre hivatkozással történt, ez a logika a terrorizmussal küzdő államokban, mint pl. Izrael, Libanon, Palesztina stb. igen jelentős érvként hangzik el. Ugyanakkor szinte észrevétlenül bekúszott a probléma azokba a társadalmakba is, amelyek az ilyen drámai konfliktusoknak nincsenek kitéve mégpedig lényegében az IKT – különösen az internet és a robotika – fejlődésének köszönhetően. Szénay Márta cikke öt ilyen technológia hatását mutatja be empirikus vizsgálatok eredményein keresztül, ahol ezek hasznosságát, illetve privát szférát érintő hatását elemezték. Ezek az igen elterjedt térfigyelő kamerák, a civil használatban levő drónok, a kereskedelmi tranzakciókban szinte kikerülhetetlen okos telefonos követési megoldások, az elsősorban bűnözési felderítéshez használt internetes megfigyelés végül a jelenleg még hazánkban nem nagyon elterjed, de dinamikájában gyorsan fejlődő biometrikus azonosítás voltak. Anélkül, hogy ezen a ponton a tanulmány eredményeinek részletes elemzésébe belemennénk, annyit érdemes kiemelnünk, hogy az empirikus vizsgálatban résztvevő 9 országból a magyar mintában részvevők ítélték meg ezeket az IKT innovációkat a legkevésbé aggodalmasnak magánszférájuk megsértésére, mégpedig a 72%-ban „aggodalmaskodó" átlaggal szemben mindössze 38%-ban, ami a minket közvetlenül megelőző Egyesült Királyság „aggódó" szintjének is alig fele. Úgy látszik, mi magyarok, nem érezzük veszélyben privát szféránkat a modern megfigyelési technológiákkal szemben…

Raab cikke azért nagyon fontos elméleti kiindulópont, mert leszámol azzal a leegyszerűsítő gondolatkörrel, hogy a magánszféra és a biztonság egyensúlya egy közgazdaságilag egy zéró összegű játék lenne, illetve amellett érvel, hogy nem fog születni fenntartható „biztonsági kormányzási modell" (governance of security), ha nem gondoljuk újra a magánszféra koncepcióját az információs társadalom kontextusában. Ennek az újragondolásnak pedig a vezérfonala abba az irányba kell, hogy elinduljon, hogy ontológiailag nem egymással ellentétes fogalmakként kell szembe állítanunk a magánszférát és a biztonság iránti igényt, hanem mindkettőnél a közjószágból kiinduló felfogást kellene alkalmaznunk. A cél nem egy „alkumodell" optimalizálása, azaz egyensúlykeresés, hanem a probléma átfogalmazása, a belső paradoxonok feloldása, illetve egy alaposabb magánszféra és biztonság fogalom használata. Raab alátámasztja, hogy ki kell, hogy tágítsuk a közérdek fogalmát oly módon, hogy egyértelműen részévé válhasson az egyéni magánszféra védelme. Ez alapján elfogadható lehet az, hogy a magánszféra védelmére irányuló követeléseket a köz érdekében – és ne ellene – fogalmazzák meg. Az IKT eszközök elterjedése szempontjából ennek azért van igen nagy jelentősége, mert a privát szférát leggyakrabban nem a „kaszárnya állam" támadja – természetesen a demokrácia szempontjából ez komoly probléma – hanem a felhasználók mindennapi viselkedése, felkészületlensége, és olyan bevett gyakorlatok, amelyek egy más technológiai paradigmához kötődnek (pl. a fizika biztonsághoz, nem a digitális lábnyomok következmények nélkül hagyásához).

A Raab cikkben felvetett elméleti koncepciókat két eredeti kutatás fejleszti tovább a különszámokban; az egyik Székely Iván, Somodi Bernadett és Szabó Máté Dániel két részes cikke, amelynek első fele a Replikában, második pedig az Információs Társadalomban olvasható, és a Privacy and Security Mirrors (PRIMS) kutatás eredményeit foglalja össze. A másik tanulmány a már említett Szénay Márta által jegyzett SurPRISE (Survaillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe) kutatást mutatja be. Elméleti szempontból mindkettő az alkumodell továbbfejlesztését célozta meg, amelyeket empirikus adatokkal igyekeznek alátámasztani.

Székely és társai a PRISM kutatás eredményeként két fontos hipotézist igazolnak. Az első az, hogy az általános biztonság és a személyes biztonság egymással korrelál, tehát a növekvő biztonság iránti igény, nagyobb igényt támaszt a magánszféra biz-

A szerző BME GTK Pénzügyek Tanszék tanszékvezető egyetemi tanára.

tonságával szemben is. Az alkumodell meghaladására utal a második empirikus eredménysorozat is, amelyik viszont nem mutat szignifikáns összefüggést a magánszférának sem a személyes biztonság igényével, sem az általános biztonsággal kapcsolatos elvárásokkal. Azaz, nemcsak elméleti megfontolások támasztják alá, hogy a magánélet autonómiájának nem alternatívája a biztonság, hanem az adatok is azt mutatják, hogy az emberek egyszerre szeretnének köz- és magán biztonságot és magánszférájukban jogot a „békén hagyásra".

A PRISM ikerkutatása, a SurPRISE további érdekes, és igen erősen kontra intuitív eredményekkel szolgál ehhez a kérdéshez. Az STS irodalomhoz fontos hozzájárulás Szénay cikkében a már korábban említett öt infokommunikációs technológiának a megfigyeléssel kapcsolatos hatáselemzése, és annak a térképnek a felrajzolása, hogy ezek az eszközök egyáltalán nem tekinthetők „fekete doboznak", mert mindegyik másképp fordítódik le a felhasználók olvasatában. Például még nem annyira elterjedt, de potenciálisan jelentős növekedés előtt álló drónokat tartják a megkérdezettek a legkevésbé hasznosnak, ugyanakkor viszont a magánszférát leginkább potenciálisan sértő innovációnak. Ezzel szemben a biometrikus azonosítást amellett, hogy hasznosság szempontjából semlegesnek tartja a megkérdezettek csoportja, a magánszférával kapcsolatos beavatkozás szempontjából viszont elfogadhatónak ítélik meg. Mi, magyarok, ezeket a megfigyelési technológiákat az európai átlagnál jóval hasznosabbnak és a magánszférával kapcsolatos veszélyeket jóval alacsonyabbnak ítéljük meg, aminek számos magyarázata lehet, ezekre a szerzőnek érdekes felvetései vannak, de azt gondolom ez mindenképp fontos kutatási irány az alkumodell hazai vizsgálatában. Az látszik általánosíthatónak, hogy azok a technológiák hasznosak, amelyek a bűnmegelőzéssel vagy felderítéssel kapcsolatosak, illetve azok nem elfogadottak, amelyekkel kapcsolatban az a veszély, hogy nem arra használják, amire eredetileg szánták őket. Ez a gondolatkör vezet át minket Székely és szerzőtársai cikkének második részére, amelyik az alkumodell meghaladásával kapcsolatban a jogi és döntéstámogatási eszközöket elemzi, és normatív irányba tereli a témával kapcsolatos diskurzust.

Székelyék abból indulnak ki, hogy az európai hagyományok alapján – a Német Szövetségi Alkotmányból kiindulva, de azon messze túlmutatóan – a jogok konfliktusát az ún. arányosság koncepciója szerint oldható fel pragmatikusan. Ezt a koncepciót tette magáévá a strasbourgi Emberi Jogok Európai Bizottsága, amely az Európai Emberi Jogi Egyezményben foglalt korlátozási klauzulákat az arányosság alapján értelmezte. A „strasbourgi módszer" a jogkorlátozás legitim céljának azonosítását, és a korlátozás szükségességének és arányosságának vizsgálatát foglalja magában. Az EJEB ítélkezési gyakorlata és az EEJE kerete alapján az arányosság teszt alkalmazását döntéstámogatási algoritmusként mutatják be, amely rendkívül pragmatikus „mérnöki" módon ad eszközt a döntéshozók kezébe az arányossági elv alkalmazására. A döntési algoritmus kérdései a jogkorlátozás céljaira, az adott megoldás alkalmasságára és szükségességére – tények alapján adott válaszokra alapoznak. A morálisan megítélhető vagy szűk értelmezésű arányossági mérlegelés a szerzők modelljében csak ezután következik, ami nagymértékben szűkíti az alkumodell „elfogultságát" azaz az érintettek jogainak indokolatlan korlátozását.

A témakör egy rendkívül érzékeny szélső értékét tárgyalja Pásztor Emese a nemzetbiztonsági adatgyűjtés kockázatainak gyakorlati problémáival kapcsolatban – konkrétan a jogi kontrollmechanizmusok hogyan tudják kezelni azt a kockázatot, hogy az állam az ártatlanság vélelmét és a konkrét bűncselekményekhez kötődő gyanút félretéve, ne tekintsen minden állampolgárra kockázati tényezőként. A szerző cikkében Székelyékhez hasonlóan konstruktivista módon javaslatot tesz egy olyan „ideális rendszer" bevezetésére, amelyik a terrorizmus elhárítására hivatott szervezetek működésének ellehetetlenítése nélkül az eljárás valamennyi szakaszában lehetőséget ad az egyén alapjogainak hatékony védelmére. Pásztor a függetlenség elvét helyezi gondolatmenetének középpontjába, és ez alapján lényegében az obudsman és a rendesbíróság intézményét ítéli meg egyedül olyannak, amelynek hatásköreit nem érintették még korlátozások.

Visszatérve a tudatos megfigyelést támogató vagy a magánszféra biztonságát sebezhetővé tevő technikai megoldások kérdéskörére, a különszámok négy cikke tárgyal olyan problémákat, amelyek kimondottan a Szénay cikk speciális IKT hatásaihoz köthetők. Ezek azok sajátos technikai és társadalmi kapcsolati kérdések, amelyek egyértelműen az innováció következményeként adódnak, és vetnek fel fontos feladatokat a szakpolitikusoknak, állampolgároknak, de az információs társadalom egyébként minden szereplőjének.

Szabó Endre Győző és Révész Balázs ebben a sajátos problémakörben az adatainkhoz való hozzáférés, az információkezelés illetve az ezekhez kapcsolódó önrendelkezés jogkörét, és az ezen a téren lejátszódó drámai változásokat elemzik. Cikkük azért nagyon lényeges, mert azzal, hogy szinte minden és mindenki valamilyen formában a kibertérben is megjelenik, ezzel a magánszférába való beavatkozás technikai végcélja az adatok megszerzésére, illetve megvédésére fókuszál. Megmutatják, hogy az adatvédelem számos eleme garantálható jogszabályokkal, deterministа technológiai megoldásokkal (pl. az e-közigazgatásban a szakrendszerek tudatos szétválasztásával, az adatok összekapcsolásának elvi lehetetlenné tételével) vagy a legkorszerűbb privátszférát erősítő technológiák (privacy enhancing technologies PET) alkalmazásával, de ezek sem garantálják azt, hogy a biztonsági incidenseknek kiszűrhető legyen az az igen magas százaléka, amit a munkavállalók, magánszemélyek hanyagsága, gondatlansága vagy egyszerűen ismerethiánya okoz.

A PET-ek fokozatos elterjedése, azok használatának elsajátítása remek példája annak az igen fontos elvnek, amelyet Kiss Attila és Krasznay Csaba vezet le a felhasználói viselkedéselemzés jogi kérdéseit tárgyaló cikkükben. Ez az elv az ún. beépített adatvédelem elve (privacy by design), amelynek lényege, hogy a magánszféra-védelem és az adatvédelmi szabályozás elveit integrálni kell a különböző adatkezelési technológiák követelményrendszerébe, így ezeknek az IKT eszközök integráns részeivé kell válnia anélkül, hogy azok funkcionalitása korlátozódna. A felhasználói viselkedéselemzés szempontjából ezek elterjesztése azért rendkívül fontos, mert az internetes üzleti modellek igen nagy része azon alapszik, hogy a használat során keletkező nagymennyiségű adat elemzésével felhasználói profilokat készít, és a termékek és szolgáltatások testreszabását, árazását, sőt kiszállítását is ennek megfelelően ajánlja fel. Igen sokszor ehhez a profilírozáshoz bizonyos előnyök érdekében önként hozzájárulunk, de annak a kockázata is igen nagy, hogy az adatgazdák/adatkezelő tudatosan vagy valamilyen külső támadás következtében kiszivárogtatják védett adatainkat. A szerzők felhívják a figyelmet arra, hogy a 2018 elején életbelépő kötelező érvényű Általános Adatvédelmi Szabályzás (General Data Protection Regulation) igen szigorú rendelkezéseket ír elő a hozzáférési jogok és az elszámoltathatóság vonatkozásában. Ennek egyik fontos technológiai feltétele a deanonimizálás, amit Gulyás Gábor György tárgyal ebben a kérdéskörben.

Gulyás cikke az Információs Társadalom folyóiratban a gépi tanulási módszerek használhatóságát mutatja be az anonimizálási probléma megoldására, azaz arra, hogy digitális lábnyomaink eltüntethetőek illetve kevésbé támadhatóak legyenek. Élénken emlékszem mennyire meglepett Kiss Attila kollégám előadása (akkor még az NKE tanársegéde volt), ahol megmutatta, hogy az irányítószám, születési dátum, és nem alapján, bizonyos esetekben milyen nagy valószínűséggel tudunk azonosítani konkrét személyeket Magyarország néhány területén. Az anonimitás, nem csak az internetes viselkedés követhetősége miatt jelentős tehát, de nyilván bizonyos fizikai folyamatok kibertérbe kerülésével itt válik olyan problémává, amelyik biztonságos megoldás nélkül lehetetlenné válik társadalmi bevezetésre. A cikk nem említi, de saját ku-

tatásaink szerint például az anonimitás kritikus kérdés ez on-line szavazások területén, a kripto valuták bevezetésében vagy a számviteli elszámolásokat automatizáló blockláncok alkalmazásában. A Gulyás által bemutatott gépi tanulási algoritmusok annak a valószínűségét igyekeznek minimalizálni, hogy tudatos támadással, rosszindulatú beavatkozással visszafejthetők legyenek adatok között kapcsolatok, pl. közösségi hálók, bankszámla adatok, egészségügyi információk és hasonló egyénekhez kapcsolható összefüggések. Sajnos ugyanis, a digitális lábnyomok, igen érzékeny és viszonylag könnyen felhasználható támadási kapuk az adathalászok számára. A gépi tanulás és a mesterséges intelligencia szoftveres algoritmusai végezetül a különszám legfuturisztikusabb, de a tudomány-technológia-társadalom kutatási program szempontjából talán legjelentősebb kérdéséhez – lényegében a robotok uralmához vezetnek el minket, amit Ságvári Bence algoritmus etikával foglalkozó cikke tár elénk.

Ságvári a magyar társadalomtudományban úttörő módon és alapossággal mutatja be két fogalomkör utóbbi években való összekapcsolódását és ezek potenciális következményeit. Az egyik a már viszonylag ismert és alkalmazott adatgyűjtés és adatfeldolgozás (a Big Data) világa, a másik az egyre dominánsabb és életünket meghatározó – többnyire ismeretlen és védett – algoritmusok világa. Gondoljunk például Sergey Brin és Larry Page Google alapítók híres-hírhedt keresőalgoritmusára, amelyik vállalatok forgalmának sorsát dönti el aszerint, hogy hova sorolja be találatukat. De ugyanilyen iparági versenyt meghatározó erejű algoritmus rejt a Tripadvisor szállodai értékelő kódja, a tőzsdei kereskedést meghatározó robotok vagy akár a nagy e-kereskedelmi cégek (E-bay, Amazon, Netflix stb.) ajánló rendszerei is. Mennyire bízhatunk ezekben a kódokban? Hogyan ellenőrizhetőek ezek a transzparencia, diszkrimináció mentesség vagy az adatvédelem szempontjából? Mennyire érzékenyek az algoritmusokat készítők ezekre a problémákra, és milyen általános társadalmi kontroll mechanizmusok építhetők be az egyre jobban terjedő – egyáltalán nem csak a repetitív, rutinszerű hanem a kognitív intelligenciát is drámai módon érintő humán képességek automatizálását célzó megoldások auditjára.

Feltétlenül ajánlom a Replika és az Információs Társadalom számát mindenkinek, akit a közeljövőnket érintő változások érdekelnek nemcsak a biztonság és a magánélet dimenziójában, hanem általánosságban is a technológia és társadalom infokommunikációs korszakban jelenlévő kihívásaival kapcsolatosan is. Kiemelten javaslom a cikkek feldolgozásra ajánlását egyetemi hallgatók, illetve a közszféra továbbképzéseiben résztvevők számára, sőt érdemesnek tartanám külön jegyzetben is a 9 cikk megjelentetését a téma fontosságát és jelentőségét tekintetbe véve.