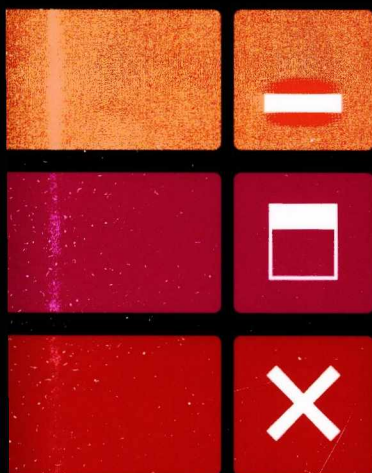


AZ

INTER- NET



a kockázatok
és mellékhatások
tekintetében

Az elmúlt húsz évben kialakult egy új, széles utakat biztosító virtuális világ, az internetes hálózatoké. Hogyan védjük meg az itt közlekedőket? Hogyan hívjuk fel a figyelmet a veszélyekre és a kockázatokra? E könyv szerzői úgy gondolják, hogy ki-ki a maga szakterületén tud valamit, amit ha elmond az internethasználóknak, segít megővni őket sok későbbi „ütközéstől”, balesettől, problémától, a kockázatoktól és mellékhatásoktól.

E könyv szerzői az önmagukért felelősséget vállaló fiatal és idősebb felnőttekhez szólnak: szülőkhöz, tanárokhöz, akik felelnek gyermekeikért, a környezetükben lévő fiatalokért és tanítványaikért, hogy segítsék őket minél kisebb kockázattal élvezni az internet nyújtotta színes, új világot. A szerzők eltérő korúak, különböző képzettségűek, írási szokásaik is eltérőek, de mindegyikük az informatika, az internet világában él és dolgozik. Éppen ezért, mint a legbeavatottabbak



AZ INTERNET

a kockázatok és mellékhatások tekintetében

A könyv kiadását

a Neumann János Számítógép-tudományi Társaság támogatta

a kockázatok és mellékhatások tekintetében

[illegible]

20. 11. 1971

Hausnummer, az este clasa 222,

© Csepeli György, Demetrovics Zsolt, Koronczai Beatrix, Rác Bence,
Szabó Endre Győző, Szabó György, Székely Iván, Talyigás Anikó,
Talyigás Judit, Turchányi Géza, Vajda Zsuzsanna, Z. Karvalics László

© Scolar Kiadó, 2010

Minden jog fenntartva. A szerkesztett szövegek egyetlen részlete sem
használható fel, nem tárolható és nem sokszorosítható a kiadó előzetes
írásbeli engedélye nélkül.

Köszönjük, hogy a Scolar Kiadó könyvét választotta

Scolar Kiadó, 2010
1016 Budapest, Naphegy tér 8.
Tel./fax: + 36 1 466-7648
scolar@scolar.hu
www.scolar.hu

Felelős kiadó: Érsek Nándor
Felelős szerkesztő: Talyigás Judit
Könyvterv, borító: Máthé Hanga

Nyomdai munkák: Reálszisztéma Dabasi Nyomda Zrt.
Felelős vezető: Vágó Magdolna vezérigazgató

ISBN 978 963 244 226 6

TARTALOM

Előszó	7
TALYIGÁS JUDIT Felvezetés	9
CSEPELI GYÖRGY Veszélyesen élni? Avagy az internethasználat kockázatai	25
SZABÓ ENDRE GYŐZŐ A személyes adatok védelmének kérdései a virtuális világban	43
RÁCZ BENCZE We watch you watch	67
SZÉKELY IVÁN Kukkoló társadalom – avagy van-e még függöny virtuális ablakunkon?	93
DEMETROVICS ZSOLT-KORONCZAI BEATRIX Az internetfüggőség néhány pszichológiai vonatkozása	121

Z. KARVALICS LÁSZLÓ Az univerzális kvantor rémuralma – avagy a veszélydiskurzusok logikai szerkezetéről	133
TALYIGÁS ANIKÓ Az informatikaoktatás dinamikája	149
VAJDA ZSUZSANNA A gyerekek és a számítógép	167
SZABÓ GYÖRGY Virtuális világ és valós tér. Utópiák, realitás, veszélyek	193
TURCHÁNYI GÉZA Tévedések vigjátéka – avagy hány internethasználó is van?	207
JEGYZETEK	219
A SZERZŐKRŐL	235
IRODALOM	241
TÁRGYMUTATÓ	253

ELŐSZÓ

Digitális Esélyegyenlőség. Sokan, sokféleképpen és sokat beszélünk e témáról, de vajon a beszélők tesznek is valamit, hogy az internet, a digitális technika használói vagy éppen a ma még ezt nem alkalmazók érzékeljék a változás lehetőségét, irányát? Miért is fontos és lassanként elkerülhetetlen ez?

A legrövidebb válasz: az információs társadalom nem szabadon választott, szeretem vagy nem szeretem kategória. Ez a valaha „szép új világ” ma már életünk mindennapja lett. E felismerés hiánya hátrányt jelent az ország és az egyén számára is.

Kicsit bővebben: Minek is a hiánya?

- annak, hogy barátságban legyünk a bennünket körülvevő eszközökkel,
- annak, hogy használni tudjuk őket,
- annak, hogy segítségükkel az életünk könnyebbé váljon,
- annak, hogy az eszközök segítségével többet, jobban és más-hogyan tudjunk törődni az egészségünkkel
- annak, hogy megváltozott, bővült a tanulás lehetősége
- annak a felismerésnek, hogy az információs társadalom korában élünk, és ennek figyelmen kívül hagyása néhány éven belül akár káoszhoz is vezethet,

– és persze annak, hogy tudatában legyünk e „szép új világ” veszélyeinek, kockázatainak is.

A Neumann János Számítógép-tudományi Társaság, az informatika legrégebbi, folyamatosan megújuló szakmai szervezete felismerte, hogy a tudás a civil társadalom iránti felelősségvállalásra kötelezi. Ezért programjában kiemelt fontosságot kapott és kap napjainkban is a Digitális Esélyegyenlőséggel kapcsolatos konkrét munka: az ismeretek különböző szintjének terjesztése, a hátrányos helyzetűek támogatása, az EGÉSZ-ség. Fontos feladatként tekintjük az emberek motiválásának, igényeik felkeltésének, ismereteik célirányos bővítésének hatékonyabbá, sőt hatékonyra tételét. Röviden: elősegíteni a digitális szakadék egy nekifutással való átugrásának lehetőségét és képességét.

Az információs társadalom nem a jövő, mára már mindennapjaink része. De vigyázat: „a fejlődés ellen nincs gyógymód” (Neumann János), ha kiengedjük a kezünk közül az irányítást, ha nem élünk kellő körültekintéssel, az rengeteg problémát okozhat. Tegyük meg közösen mindent ennek elkerülésére. E gondolatok jegyében támogatta szervezetünk e könyv megjelenését is.

Alföldi István
Ügyvezető igazgató
NJSZT

Talyigás Judit *Villamosmérnök, politológus,
az MTI Zrt. Adatbázisok és Archívumok vezetője,
az információs társadalomhoz kötődő több könyv
szerzője vagy szerkesztője*

FELVEZETÉS

Ez a könyv azért készült, mert többen úgy gondoljuk, a tudás felelősség.

Ha a meteorológus tudja, hogy orkán, tornádó közelít, kötelessége szólni, és az érintettekhez ezt a hírt minél gyorsabban eljuttatni, hogy módjuk legyen felkészülni. Ha az autógyár rájön egy hibára, akkor kötelessége visszahívni az autókat a Föld bármely pontjáról, hogy megóvja az autót használókat az esetleges balesetektől. Ha az orvos ismeri egy adott betegség megelőzésének módját, akkor felhívja erre környezete figyelmét, sőt az elhivatottabbak ismeretterjesztő előadásokat tartanak, hogy szűrésekre jártanak az emberek.

Az élet különböző területein léteznek ismertebb vagy kevésbé ismert kockázatok. Ezeket fel kell ismerni; aktív tevékenységgel csökkenthetők is a kockázatok, elkerülhetők a balesetek, katasztrófák. Ilyen tevékeny megelőzés a gátépítés éppúgy, mint a rákszűrés.

Van más jellegű védelem is. Ahol lehet, ott a szakma és a jog kialakít egy jól meghatározott, betartandó szabályrendszert. Így védi például a közlekedőket a KRESZ. Gondoljunk csak bele: a Föld egyre több, egyre szélesebb útjain egyre több autó, kamion közlekedik, ennek ellenére nem emelkedik a balesetek száma, hanem csökken. A Földön szinte egységes KRESZ-szabályok betartásáért mind többen tesznek a közlekedési szakemberek. Szabadon és biztonságosan utazni a legjobb dolgok közé tartozik. Az elmúlt húsz évben kialakult egy új, széles utakat biztosító virtuális világ, az internetes hálózatoké. Hogyan védjük meg az itt közlekedőket? Megfelelő módon felhívjuk-e a figyelmet a veszélyekre és a kockázatokra?

E könyv szerzői úgy gondolják, hogy ki-ki a maga szakterületén tud valamit, amit ha elmond az internethasználóknak, segít megóvni őket sok későbbi „ütközéstől”, balesettől, problémától. Könyvünk azért született, mert meggyőződésünk szerint az internet ma már az életünk része, sok öröm és hasznos lehetőség forrása, amiről nem szabad lemondani. Ezzel együtt az internethasználat sok váratlan, ismeretlen kockázatot is jelenthet, amelyekről beszélni kell, amelyeket ismerni kell.

Ezzel a szándékkal nem vagyunk egyedül. Az Európai Unió Safer Internet Plus¹ programja felvilágosító és tájékoztató anyagokkal segíti elsősorban a gyerekeket. Hazánkban egyebek mellett a Neumann János Számítógép-tudományi Társaság (NJSZT) konferenciákkal, szakmai anyagokkal és e könyv megjelenésének támogatásával is segíti a tudatos internethasználatot, a váratlan veszélyek elkerülését az internet mindennapi használatakor.²

E könyv szerzői nem a gyerekekhez, hanem az önmagukért felelősséget vállaló fiatal és idősebb felnőttekhez szólnak: szülőkhez, tanárokhoz, akik felelnek gyermekeikért, a környezetükben lévő fiatalokért és tanítványaikért, hogy segítsék őket minél kisebb kockázattal élvezni az internet nyújtotta színes, új világot.

A szerzők eltérő korúak – egyesek húszas éveik végét, mások hatvanas éveik elejét tapossák. Hétköznapi életük is különböző: van tisztviselő, jogász, tanár, pszichológus, orvos, mérnök és szo-

ciológus. Így van, akit a reggel a hivatalban, mást az iskolában, egyetemen köszönt. Némelyek gyerekek, fiatalok között élnek, dolgoznak, mások hivatali dokumentumokkal és izgatott ügyfelekkel színesítik életüket. Írási szokásaink is eltérőek, de mind egyikünk az informatika, az internet világában él és dolgozik. Éppen ezért mint a legbeavatottabbak szólunk szeretettel és aggodalommal e témáról.

Természetesen stílusunk is különbözik. A jogászi zsargon vagy az orvosi, szociológusi, esetleg műszaki szakszavak nem ígérnek könnyű olvasmányt, az eltérő megfogalmazások azonban színes ízelítőt nyújtanak az internettel együtt élők világából. A szerzők között van, aki a válságok és veszélyforrások halmozódása miatt kevésbé látja biztatónak a jövőt, míg mások a lehetőségek széles skálájára hívják fel az olvasó figyelmét. Ez utóbbit teszem én is. Van, aki úgy véli, hogy „a jó győzelmenek előfeltétele a rossz megismerése”. Ezzel egyetértve szeretnénk, ha a jövőben az internet segítségével további új csodák és lehetőségek nyílnának újfajta közösségi kapcsolatokkal az olvasók előtt.

A mindennapok embere számára az internet széles körű elterjedése és minél gondtalanabb élvezete, a tanulás, szórakozás, információcseré és az új felfedezésének korlátlan lehetősége jelenti, jelentheti a jót.

Remélem, a kedves olvasó talál az ízléséhez közel álló stílust, érdekes témát. A könyv egyes fejezetei a technika természetéből fakadó veszélyeket is ismertetik, nagyobb hangsúlyt kap ugyanakkor a személyi adatok védelmének, az internetfüggőségnek, a hacker fogalmának és szerepének, a gyerekek, fiatalok és az internet viszonyának kérdése, valamint a személyes kiszolgáltatottság és az általánosítás kockázata. Külön fejezet foglalkozik a térinformatika elméletével, fejlődésével és kockázataival. Az egyes fejezeteket nem kell sorrendben olvasni, de érdemes mindet elolvasni, hiszen más-más szemszögből látják a szerzők a világot és benne az internethasználatot, pontosabban annak kockázatait. Érdekes megfontolásokkal és/vagy szakmai tanácsokkal lehetünk gazdagabbak olvasás után.

Az internettel keresztül-kasul hálózott világunk kockázataiból mutatunk be területeket a teljesség igénye nélkül, a figyelemfelhívás, az önszabályozás kialakulásának elősegítése érdekében. Ez kiszolgáltatottságunk kockázatának jelentős csökkenését eredményezheti. Mint Csepeli György fejezete érzékelteti: sok más kockázat is létezik a Földön, amelyekről tudnunk kell, s amelyek összegyűjtött bemutatása talán segíti az internet kockázatának helyesebb értékelését is.

Életünk változása

Évszázadokkal ezelőtt csak kevesek kiváltsága volt az írás és az olvasás tudása. Az emberiség történelmében kiemelt jelentőségűek az első írásos emlékek; hasonlóképpen fontos számunkra az első magyar nyelvű emlék. Az írás a hatalom jelképe volt. Később, a Gutenberg-galaxisban úgy éltünk, hogy tudtuk: ami nyomtatásban megjelent, azt komolyan kell venni. Hiszen csak az jelenhetett meg nyomtatásban, amit a szerzőn kívül elolvasott a lektor, a szerkesztő, és amit végül kiadásra alkalmasnak találtak. Ez jelentette az anyagok szakmai megbízhatóságát és a megjelenés korlátozását is. Mind a könyv, mind az újság kollektív munka eredménye volt.

Az internet elterjedése megváltoztatta napi szokásainkat. A XX. század vége előtt gondolatainkról, utazási élményeinkről telefonon vagy levélben számoltunk be barátainknak. Az internet megjelenése lehetővé tette, hogy a körülöttünk zajló eseményeket barátainknak elektronikus levélben (e-mailben), vagy ha többeknek szánjuk, blog formájában írjuk meg. A jelentősebb események online hírekben, videóban kerülnek ki a portálokra. Így az internet a civil világ információcseréjének is területe lett. Más megfogalmazásban: olyan esemény, tény is közkinccsé válhat, amely az internet előtti időszakban csak szűk baráti, családi körök ismerete volt.

Ez a változás új lehetőség: újabb és újabb kutatási területet kínál különböző szakterületek kutatóinak, ismerőinek. Victor Ga-

laz, a Stockholmi Egyetem munkatársa, kutatási vezető 2010 márciusában egy Oslóban tartott konferencián elmondta: olyan automatikus szűrőrendszereket fejlesztettek ki, amelyek adott témakörben célzó keresőkkel és adatgyűjtéssel az interneten elérhető jelentéktelen adatokból nagyobb, teljesebb képet állítanak össze. Példái olyan események teljesebb megismerésére utaltak, mint az olajszennyezés, az erdők kipusztulása vagy a túlhalászás. Létezik egy hasonló kanadai fejlesztésű program (Global Public Health Intelligence Network, GPHIN),³ amellyel betegségekről gyűjtenek össze nagy sikerrel információkat a világhálóról. „A GPHIN találja meg évente a 40 százalékát azoknak a jeleknek, amelyek elsőként utaltak az Egészségügyi Világszervezet által később vizsgált és bizonyított 200–250 járványra” – hangsúlyozzák a *Frontiers in the Ecology and the Environment* című szaklapban megjelent tanulmány szerzői.

Azaz minden elérhető és felhasználható, ami a hálón megtalálható. Az előbbi példák jó és hasznos célokról szólnak.

De vajon mi mindenre használható az adatgyűjtés és az eredmények összerendezése, ha személyes adatokról van szó? Erről szól elsősorban Szabó Endre fejezete, de érinti a témát Székely Iván és Rácz Bencze is.

Az emberi kapcsolatok és az internet

Az 1970-es évek végén, az 1980-as évek elején, a számítógép megjelenésének és elterjedésének idején többünket izgatott az a kérdés, hogy melyek azok a témák, amelyekről könnyebb beszélni a számítógéppel szemben ülve, és melyekről természetesebb emberek közötti személyes kapcsolatban. Azt gondoltuk, lehetnek olyan betegségek, amelyek tüneteit egyesek nehezen mondják el szemtől szemben, s előre megfogalmazott kérdésekre őszintebben válaszolnak, kevésbé jönnek zavarba, mint ha egy orvos teszi fel ezeket a kérdéseket. Kísérletek folytak a számítógépes vizsgáztatás lehetőségéről is, gondolván, hogy objektívebb lesz a tudás mérése,

ha azt nem zavarja a vizsgáló és a vizsgáztató egyénisége. Ezzel egy időben felvetődött az a kérdés is, hogy milyen munkafolyamatok számítógépes támogatása segíti az emberi munkát például az önkormányzatoknál. Hol van a gépesítés határa? Hol szükséges az emberi döntés, amely gépesítéssel nem váltható ki? Ez utóbbi kérdéssel még az 1990-es években is foglalkoztak Vámos Tibor akadémikus vezetésével a Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézetében, a SZTAKI-ban. Az 1990-es években több kísérlet folyt, amikor a beteg az orvosi rendelőben használhatta a számítógépet, és a vizsgázók is válaszolhattak az egyetem adott termében a kérdésekre. A XXI. század elejére a helyzet gyökeresen megváltozott. Egyedül vagyunk a számítógéppel – ha a kérdést, a választ nem értjük, nincs jelen szakember, akivel konzultálhatnánk. A XX. században, ha az orvosi rendelőben ülő betegnek feltett számítógépes kérdés nem volt elég egyértelmű, ha a diák nem értette az oktatóteremben számítógépen olvasott vizsgakérdést, megkérdezte, megkérdeshette a jelen lévő orvost, vizsgáztatót.

Az internet megjelenése és széles körű elterjedése e területeken is változást hozott. Megjelentek a weben azok az orvosi, egészségügyi, oktatási szolgáltatások is, amelyek azért készültek, hogy ha egyedül vagy és segítségre van szükséged, hozzájuk fordulhass.

Így némi böngészés vagy baráti, ismerősi tanács alapján találhatunk olyan portálokat, ahol lehetőség van lelki-tesztijainkra reményeink szerint szakmailag megbízható és megfelelő választ kapni. E portálokon saját nevünkön bemutatkozva panaszoljuk el testi problémáinkat, szerelmi vagy gyereknevelési, esetleg még bensőségesebb lelki gondunkat. Bízunk abban, hogy a másik oldalon hozzáértő és orvosi, jogi titkot megtartó ismeretlen ül. A folyamatos „beszélgetés”-hez, a megfelelő válaszok megadásához szükséges, hogy a válaszadó levelezésünket archiválja, könnyen előkereshetően tárolja. Ezekben az esetekben azonban többnyire saját néven, címen jelentkezünk be. Az orvosoknak, a jogászoknak mély bizalmat szavaztunk a való világban, és a virtuális térben is tovább él ez a bizalom. A különbség csak annyi,

hogy itt a technikai tér megbízhatóságát nem ismerjük. Hisszük, és nem tudjuk, hogy a válaszadó valóban megfelelő képzettséggel rendelkezik.

A web új technikai lehetőségeket nyit számunkra, hogy ismeretlenekkel álljunk szóba, és megosszuk velük gondolatainkat. Ennek több formájáról is érdemes beszélni: elsőik között a párkereső és – szerencsés esetben – pártaláló oldalakról. Itt a rutinosabbak álneveken, álcímeken, mégis saját magukat adva beszélgetnek, randevúznak a virtuális térben. Ennek veszélyeiről sokan írtak és nyilatkoztak már. Véleményem szerint a kockázat éppen annyi, mint a való világban. Nincs nagyobb, de kisebb bizalom sem új kapcsolat építésében attól, hogy a való világ „helyett” a virtuális téren keresztül találkozunk.

Ha a valódi világban meg szeretnénk ismerni egy másik embert, mielőtt bárhova elmennénk vele, akkor látszólag előny, hogy látjuk és halljuk, és ebből következtethetünk megbízhatóságára. Ez a virtuális világban is így van, csak éppen egyedül ülve a számítógép mögött többet lehet kérdezni, és – talán – könnyebb őszintén válaszolni. De a virtuális tér éppúgy megtűri a hazug válaszokat, mint a valódi, és kiszűrésükre a kérdezőnek kell elég felkészültnek lennie. Tudni kell, miről és kinek beszélünk, s eldönteni a válaszok megbízhatóságát.

Én nem szeretnék bizalom nélküli világban élni. A netes világban is a józan bizalomra szavazok. A józanság érdekében született ez a könyv.

Az új emberi kapcsolat kialakításának egyik meghatározó lehetősége a közösségi oldalak megjelenése. Jó megtalálni rég elveszettnek hitt barátainkat, vagy éppen könnyedén – telefon, postaköltség nélkül – csevegni ismerőseinkkel, akár egyszerre többel is. Nem érdekes, hogy éppen ki hol tartózkodik, virtuális terünk közös. Mégis egyre többen – könyvünkben Szabó Endre, Rácz Bencze és Talyigás Anikó – felhívják a figyelmet e közösségi oldalak használatának kockázataira, arra, hogy figyeljünk arra, mire és hogyan használjuk. Ám ez természetesen nemcsak magánszemélyeknek jelent nagy lehetőséget. A szociológusok szá-

mára ritka terepet jelentenek a kapcsolati hálózatok tanulmányozására, és más, nem civil szervezetek számára is sok információt tartalmaznak a mind taglétszámukban, mind szolgáltatásaikban egyre bővülő közösségi oldalak.

Az internethasználat jelentősen megváltoztatja egyebek mellett a tanár–diák viszonyt, amint erről Talyigás Anikó is ír. A diákok kérdéseikkel és kéréseikkel könnyebben fordulnak a tanárhoz, mint régen, amikor még a tanári szoba előtt kellett várakozniuk. Az egyetemi hallgatók óraáthelyezési kérései, utólagos tananyagkérelmei szinte természetesek. A tanulók, mint majd olvasható, tanulásra fordítják a legkevesebb internetezési időt.

A net mint a tájékozódás alapforrása

Az értékesebb szakdolgozatok, szakmai anyagok bibliográfiai hivatkozásokat tartalmaznak. Régen természetes volt, hogy a könyvtárban kutakodtunk, használtuk a szerzői és tematikai nyilván tartásokat. Aztán a könyvtárhoz fordultunk, ha a szerző nem jutott eszünkbe, vagy az adott tematika alatt nem találtuk a bennünket érdeklő szakkönyvet. Ma, amikor leülünk a számítógép elé, és egy adott téma feldolgozását segítő böngészünk, megtaláljuk mindazt, amit valaki feltett a netre. Pontosabban azokat a dokumentumokat, amelyeket nem jelszóval, tűzfallal védett, esetleg fizetős, zárt adatbázisokban tárolnak. Másképpen fogalmazva: mindazt, amit az általunk használt kereső a szabadon elérhető anyagokból megtalál.

Tudnunk kell, hogy az, amit megtalálunk az adott témában, az emberi ismeretnek, tudásnak esetleg csak egy töredéke, de gyakran ez is oly sok, hogy csupán elenyésző részének feldolgozására vállalkozunk. Nem érzékeljük a hiányt. Ez a kiválasztott rész gyakran a kereső által felállított sorrend, azaz az ajánlott első tíz, húsz, esetleg negyven forrás áttekintése, feldolgozása. Varga Csaba filmrendező azt írta, hogy a múlt kutatói, a történetírók csak azokból az emlékekből, dokumentumokból, tárgyi bizonyíté-

kokból építkezhetnek, amelyek fennmaradtak. Ha a kutatás során valamilyen új tárgy, írás kerül elő, változik az elképzelésünk az adott időszakról. Így van ez akkor is, ha csak az internetről tájékozódunk, azzal a különbséggel, hogy az adott témában a való világban – könyvtárakban, levéltárakban – még számos dokumentum kapcsolódhat a keresett témához.

Az egyoldalú adatgyűjtés különösen veszélyes akkor, ha szakemberek megítélése múlik ezen. Amikor tájékozódunk valakiről az interneten (lásd részletesebben ennek kockázatait Szabó Endre fejezetében), azt hisszük, mindent megtudtunk róla, és ennek alapján döntünk. Nem feltételezzük, hogy több tény hiányzik, vagy nem valódi adat olvasható az interneten, egyre inkább csak az a fontos valakivel kapcsolatban, ami róla ott, a virtuális térben megtalálható.

A veszélyes általánosítás lehetőségének is tág teret ad az internet. Erre Vajda Zsuzsa is felhívja a figyelmet Hammer Ferenc publikációjára hivatkozva, míg Z. Karvalics László részletesen tárgyalja ennek kockázatait.

Ki mit lát az interneten?

Életünk része a számítógép. Ülünk és dolgozunk, böngészünk. Olyan, mintha egyedül lennénk. Aztán beszélgetni van kedvünk egy fórum, egy közösségi oldal, esetleg egy játékporthál vagy a Skype segítségével, és máris olyan, mintha nem egyedül ülnénk a szobában. Soha ilyen széles választék nem állt rendelkezésre az egyedüllét feloldására. A közösségi oldalon természetesen nemcsak azt látom, amit én szeretnék, hanem – valahogy úgy, ahogyan az utcáról behallatszik a zaj – sok mást is. Véleményeket ismert és ismeretlen emberekről, felhívást programokra és szövetségkötésre, esetleg önbíráskodásra (lásd Talyigás Anikó és Z. Karvalics László írásait kötetünkben).

De vajon észrevesszük-e, ha rólunk írnak valamit, ami nem felel meg a valóságnak? Vajon van-e módunk érdemben helyreigazítani azt?

Az internet mint az örökkévalóság lehetősége – vagy mégsem?

A XXI. század első éveiben egyre többen hittek az internet két nagy lehetőségében: a kultúra mindenki számára elérhető lesz, és amit egyszer feltettünk a netre, az örökké megmarad.

Ez utóbbi elképzelésnek két fő problémája van: az, ha valóban örökké fennmarad – és az, ha nem. Mint arra Szabó Endre és Z. Karvalics László is rámutat itt közölt írásában, olyan adatok is megtalálhatók a neten, amelyek már rég nem valóságok – beosztások, bírósági ítéletek, törvények, életrajzok, kutatási eredmények, nem ajánlott gyógymódok, elavult hírek, és még sorolhatnánk. Nagy tudás, ismeret kell ahhoz, hogy az internethasználó szétválassza az érvényest a már nem igaztól. A munkát nehezíti, hogy az esetek döntő részében a megtalált anyagoknál nincs feltüntetve sem időpont, sem forrás. A másik gond, mint erre Csepeli György is utal, a technika változása. A régi gépekkel nem mindig olvashatók az új anyagok. A régen feltett, féltett családi fotók, filmek, zenék eltűnnek, eltűnhetnek a CD, DVD és pendrive hordozókról is. De a családi számítógép lecserélésére is gyakran akkor kerül sor, amikor a winchester „meghal” – magával víve legszebb emlékeinket.

A XX–XXI. század történelemkutatói számára bizony lesz egy fekete lyuk, mert a fiókokból már csak nagyon kevés családi fotó és levelezés kerülhet elő.

Természetesen a nagy projektek keretében történő digitalizálások esetén a jelentős gyűjtemények kezelői több szerveren tárolják az értékes anyagokat, védve ezeket a technikai, természeti veszélyektől és az emberi gondatlanságtól. A technika fejlődésével, ha lehet, majd új formátumra konvertálva és korszerű keresőkkel teszik elérhetővé a digitális gyűjteményeket. Ezen adatbázisok jelentős része azonban zárt.

A másik kérdés, hogy a kultúra valóban mindenki számára elérhetővé válik-e az internet segítségével. A múzeumok és más közgyűjtemények a rendelkezésükre álló forrásoktól függően digitalizálják gyűjteményeik darabjait, és teszik – részben – elérhetővé a neten. A gyűjtemények feldolgozása részint a sajátos szakmai

zsargon ismeretével kereshető, más része a közember számára is rendelkezésére áll. Kérdés, ha az iskolai feladathoz Leonardo da Vinciről kell írni, sokat segít-e, ha képei, szobrai, műszaki tervei megtalálhatók és megnézhetők az interneten. Bizonyára igen. Mégis féltő, hogy mindaz az élmény, amely egy múzeumi látogatás kapcsán érezhető, elmarad. Igaz, a keresett tárgyak együtt – gyakran – csak az interneten láthatók. Ennek előnyét és nehézségét élvezzük, tudva, hogy csak úgy, szépséges tárgyat cél nélkül ritkán nézegetnek a netezők (lásd Csepeli György fejezetét).

Magány helyett internet?

A számítógép, az internethasználat, mint arról már szóltam, természetesen lehetőség a magány feloldására. Mert a magány, ellentétben az egyedülléttel, nem jó. Ha anya nem jön társasjátékot játszani, ha a haverok elmentek focizni és nekem nincs kedvem, ha bizonyítani akarom magamnak, hogy többre vagyok képes, mint mások gondolják, ott a számítógép, ott az internet. A gépen, az interneten egyaránt megtalálhatók az ártatlan, a képességfejlesztő, az agresszív, a tudást adó és a hamis világképet építő játékok. Ki választja szét ezeket? Játsszom és nyerek, látom, ahogy egyre jobb az eredményem. Késő van, de az új, ismeretlen barátok szívesen játszanak, beszélgetnek velem, mert a Föld másik felén éppen reggel van. Tér és idő összerosódik. Jó ülni a gép-nél, de hány éves kortól? Mennyi ideig? Mi az, ami hasznunkra válik? Mi az, ami ártatlan szórakozás, és mi az, amivel ártunk magunknak, ha egyre inkább együtt élünk a számítógéppel? Ezekkel a kérdésekkel is foglalkozik Demetrovics Zsolt és Vajda Zsuzsa kötetünkben. Egy, az Egyesült Államokban készült felmérés szerint egyre gyakoribb, hogy a családtagok előbb megnézik a számítógépeiken a leveleiket, arra válaszolnak, aztán ki-ki leül reggelizni. A közösség a virtuális világ lett a valós helyett. A Facebook külön gyerekközösségi oldalt hozott létre a 12 éven aluliak számára. Védelem ez, vagy üzlet?

Az internet és etika

Mit szabályoznak a jogászok? – tehetnénk fel a kérdést. A már létező valóságot, vagy előre feltételezett lehetséges eseményeket, szituációkat? Mennyire szabályozott jogilag a virtuális világ? Bűn-e, ha – mint arról az MTI hírt adott – egy közösségi virtuális játékban (Maplestory) a feleség, megtudva, hogy digitális férje elvált tőle, megöli virtuális férjét. Játék, mondhatjuk, nem több. De hol a határ? – kérjük. Az idézett hír szerint a japán bíróság komolyan veszi és elítélheti a játékost a való világban a virtuális büntetért. „A rendőrség elmondta, hogy miután az asszony illegálisan hozzájutott a férjét alakító játékos bejelentkezési adataihoz, megölte annak karakterét. A zongoratanárként dolgozó hölgy Szapporo város fogházában várta 2009-ben, hogy megtudja, szembe kell-e majd néznie az illegális számítógép-használat és adatmanipuláció vádjával.”

A jog bünteti a levéltitok megsértését. De ki figyel oda, hogy hányan olvassák el mások elektronikus leveleit, mert éppen nyitva volt a gépük, amikor arra jártak, vagy mert mint rendszergazdák könnyedén és véletlenül beletekinthetnek? Miért hiszik sokan, hogy munkahelyükről munkaidőben korlátlanul folytathatnak az interneten magánlevelezést? Írt-e vajon valaha bárki céges papírra magánlevelet, és adta-e fel a cég költségén?

A közösségi oldalakon, fórumokon, blogokon magánszemélyekről, közszereplőkről, eseményekről, árukról, szolgáltatásokról lehet véleményt írni bárkinek. Nincs más kontroll, csak az önszabályozás, hogy az igazat, a valóságot írjuk. Talán ennél többről van szó, a virtuális világban könnyebb valakit hírbe hozni – csak néhány kompromittáló képet kell feltenni a netre –, s már is tönkretettünk egy reménybeli állást vagy szerelmet. Nem lehet s nem szabad mindent a joggal szabályozni. A virtuális világban a kiszolgáltatottság veszélyeit érzékelteti többek között Rác Bencze, Szabó Endre, Z. Karvalics László és Székely Iván egy-egy itt közölt írása.

Az internet mint a „XXI. század szervezőirodája”

A XVI. században Bakócz bíborost kérte fel a pápa a keresztes hadjárat megszervezésére, aki ennek érdekében Rómából hazatért Magyarországra. A hírhozáshoz és a szervezéshez a pápai megbízottnak hosszú utat kellett megtennie. Amikor Bush elnök a XXI. század elején elhatározta Irak lerohanását, a hír a médiának, ezen belül az internetnek köszönhetően pillanatok alatt elterjedt. A szervezés természetesen még hónapokat igényelt.

A net, a közösségi oldalak rendszere hihetetlen szervezőkészségről tanúskodik. Barack Obama elnökké választását a neten szervezett támogató közösségnek tulajdonítják – joggal. De nézzünk egy közelebbi példát. 2010 nyarán a magyarországi árvízkárosultakért több mint százezren csatlakoztak a közösségi oldalakon – „cirkusz helyett kenyeret” – ahhoz a felhíváshoz, hogy az augusztus 20-i ünnepi tűzijáték helyett inkább az árvízkárosultak megsegítésére fordítsa a kormány a rendelkezésre álló forrást. A közös akarat gyors és látványos kifejezése valószínűleg meg, de nem biztos, hogy értelmesen. Hivatkozhatok Z. Karvalics László fejezetére, aki éppen e „jó vagy nem jó” általánosítások ellen lép fel.

Az internet mint közösségszervező erő komoly segítséget is nyújthat. Az Interpol INFRA-RED 2010 elnevezéssel nemzetközi körözési akciót hirdetett meg, melyre 2010. július 5. és 31. között 29 ország rendőrségének részvételével került sor. Az INFRA-RED (International Fugitive Round-up and Arrest) akció a nemzetközileg körözött szökevények felkutatására és elfogására összpontosító művelet a média, az internet bevonásával. Ilyen jellegű akcióra először 2009-ben került sor Ausztrália, Belgium, Kanada, Kolumbia, az Egyesült Királyság és az Egyesült Államok részvételével. Miután ebben a műveletben nem kevesebb, mint negyvenöt kiemelt bűnözőt sikerült felkutatni és elfogni, az Interpol főtitkársága 2010-ben is meghirdette az INFRA-RED műveletet.⁴

Mindennapjaink kockázataiból

Életünk természetes részévé vált a pendrive. Zsebünkben, táskánkban, pénztárcánkban lapul egy-kettő vagy akár több is belőle. Itt tároljuk szeretteink fényképeit, konferencia-előadásokat, legfrissebb szakmai munkánk eredményeit; rosszabb esetben viszont cégünk elemzésre váró pénzügyi adatait, esetleg az elkövetkező évek szakmai terveit vagy még nem szabadalmaztatott értékes feljegyzéseket.

A pendrive eredendően adathordozónak készült, és nem tárolónak. Mégis zokon vesszük, ha nem elég szabályosan kezelve a pendrive-ot, felmondja a szolgálatot, és örök titokként megtartja a rábízott adatokat, leírásokat, képeket. Természetesen ennél rosszabb eset, ha zsebünkéből kirántva, táskánkából kiejtve eltűnik. Csak a legmegszállottabb adatvédő szakemberek között található olyan, aki a pendrive adatait jelszóval védené. Így ha kicsit is kíváncsi ember találja meg a számunkra különösen értékes adatokat tartalmazó eszközt, elég bedugnia a számítógépébe, és könnyedén olvasható, megnézhető számára minden ott tárolt adat. Ezeknek az adatoknak, szakmai anyagoknak, személyes dokumentumoknak a nagy részét számítógépeinken sűrűn cserélt titkos kódokkal védjük. A többi kockázat sűrítmenyét adja Csepeli György írása, amelynek egyes témáit külön fejezetben is kibontottuk e könyvben.

Mire is használjuk az internetet?

Az internet természetes része életünknek – mondjuk. De mire használjuk? Kapcsolattartásra, azaz chatelünk, twitterezünk, közösségi oldalakon böngészünk, no és levelezünk, telefonálunk és blogot írunk, felhívásokat teszünk közre, játszunk és híreket olvasunk, tájékozódunk programokról, időjárásról vagy utazási lehetőségről, természetesen zenét hallgatunk és filmet töltünk le, kis idő jut tanulásra, és vásárolunk is. Ez utóbbi kockázatáról ír a legtöbbet a média. A való világ termékei és szolgáltatásai inter-

neten is elérhetők. Így hasonlóan kell döntenünk a termékek, eladók, pénzügyi tranzakciók ellenőrzésének szükségességéről vagy a bizalom megszavazásáról.

A felsorolásban szerepelt a tájékozódás. Ennek két igen eltérő területe van: az egyik esetben a szolgáltatásokról, termékekről gyűjtünk adatokat, a másik esetben a földrajzi tájékozódás új, az internet által biztosított lehetőségéről van szó. Utazunk, „megkérdezzük” a számítógépet: merre menjünk. Milyen útvonalat ajánl? Barátaink üdvözlétüket küldik egy távoli világból? Már virtuális földgömbünkön megnézhetjük közelről a várost, talán az utcát is, ahol járnak. A térképek sokat mesélnek és sokat elárulnak történelmünkéről – állította a Brit Királyi Haditengerészet volt kapitánya, régi térképek kutatója és elemzője, Gavin Menzies. E kutatás eredményei szerint a kínaiak előbb jártak Amerikában, mint Kolumbusz Kristóf az európaiakat képviselve. Mit árul el, mire jó a térinformatika, amelynek szolgáltatásai szintén hozzátartoznak mindennapjainkhoz? Erről szól többek között kötetünk lapjain Szabó György írása.

Statisztikák a netről

A könyvben idézett statisztikai adatok – elsősorban a számítógép és az internet hazai elterjedéséről – valós tartalmáért az adott fejezet szerzői felelnek. De tudnunk kell, hogy az idézett számok mögött a vetítési alapok eltérőek, a felmérés időpontja más és más, és sok egyéb tényező miatt nem tűnnek következetesnek. Például Vajda Zsuzsanna egy esetben csak az óvodás gyermekeket nevelő családokra vonatkoztatja a háztartásokban található számítógépek számát, amíg mások az összes hazai háztartásra. Fontos figyelni arra, hogy kezdetben elsősorban háztartásonként tartották ezt számon, amíg ma már egyre inkább személyhez kötött eszközökről beszélhetünk. A háztartásokra vonatkozó felméréséknél nem számított – különösen kezdetben –, hogy hány gép van, csak az, hogy van-e számítógép, illetve később, hogy

van-e internet. Ma már a háztartások jelentős részében több számítógép is található, továbbá a háztartáshoz kötött internetet kiegészíti az iskolákban, egyetemeken, munkahelyeken és közösségi térben elérhető internetezési lehetőség is. Így ma már a statisztikai felmérésekben fontosabb kérdés a használat, mint az eszköz megléte. Az internethasználat statisztikai kérdéseiről szól Turchányi Géza írása.

Csepeli György *Szociálpszichológus, az ELTE egyetemi tanára, kutatási területe a csoportközi viszonyok szociálpszichológiája, az új infokommunikációs technológiák társadalmi és lélektani hatásai*

VESZÉLYESEN ÉLNI? AVAGY AZ INTERNETHASZNÁLAT KOCKÁZATAI

Az internet az emberiség történetének új korszakát nyitotta meg. Az új korszak joggal nyerte el az „információs” jelzõt. Az információ létrehozása, tárolása, továbbítása, közlése az internet rohamosan fejlődõ teljesítõképessége és terjedése jóvoltából a XXI. századra univerzális társadalmi valósággá vált. Mint minden új korszak, az információs korszak sem szüntette meg, hanem radikálisan átalakította a megelõző korszakok társadalmi valóságát, kibontva és kiterjesztve az emberben szunnyadó képességeket, aminek révén teljesen új humánökológiai környezet jött létre. Az átalakulásnak ma még csak az elején tartunk, ezért korántsem mondható meg, hogy milyen lesz a jövõ internete által formált világ. A tévedés kockázata nélkül kijelenthetjük, hogy a korábbi korszakokhoz képest az internet szinte teljesen feloldja az információ terjedése elé állított idõ- és térbeli korlátokat.

Azt tudjuk, hogy milyen volt a világ az internet eljövetele előtt. Amióta az ember a földre lépett, minden korban folyamatos volt a konfliktus az emberben szunnyadó információs erők és az adott kor által elérhetővé tett információs viszonyok között. Az információs, a számítógépes kor előtt az emberek meg tudtak küzdeni ezzel a konfliktussal, amely nem emésztette el létezésük alapjait. A következőkben az információs kor egyes kihívásaival foglalkozunk, amelyekről ma még nem tudhatjuk, hogy a konfliktust destruktív vagy konstruktív irányba terelik. Az ember mint nem egyedeiben és az egyedek között keletkeztetett szinkron és diakron kommunikációs hálózatokban potenciálisan mindig több információt tudott létrehozni és tárolni, mint amennyit az információs viszonyokat meghatározó kommunikációs architektúrák (élőszó, írás, analóg – például nyomtatott – tömegkommunikáció) lehetővé tettek. Az új infokommunikációs technológiák esetében a veszély abban áll, hogy az architektúra, a technika „többet tud”, mint a benne részt vevő egyedek és hálózatok. Az ebből adódó veszélyeket kívánjuk sorra venni.

A bizonytalanság mindig is jelen volt az ember életében. A kezdetekben a természeti bizonytalanság tereiben merültek föl a túlélés problémái, amelyeket az emberek az adott kor információs viszonyainak megfelelően kezeltek, s vagy sikerült a problémát megoldani, vagy nem. Persze korántsem állítható, hogy egyedül az információs viszonyokon múlt a probléma megoldása, mindössze arról van szó, hogy az információs viszonyok fejlettsége az adott korban az adott probléma (járvány, babona, rémhírek terjedése stb.) megoldását sietthette vagy lassíthatta. Pragmatikus szemszögből azt lehet mondani, hogy a mérleg végül is pozitív, hiszen az emberiség minden katasztrófa és nehézség ellenére láthatóan betöltötte a Teremtő parancsát, szaporodott, sokasodott, uralma alá hajtotta a földet. A parancs civilizációs értelemben teljesült. A természet adta bizonytalanságoknak való kiszolgáltatottságunk csökkent. Az emberi lét anyagi mutatói jelentősen javultak. Eltűntek az emberek tízezreit pusztító járványok, az emberek többsége tiszta vizet iszik, fűtünk a megfagyás, megfázás

ellen, és hűtünk a meleg ellen, kényelmesebb lett az élet, megnőtt az átlagos életkor.

A civilizáció előrehaladtával vált világossá, hogy a bizonytalanságoknak volt egy másik típusuk, amelyek forrása nem a természet, hanem a társadalom. Paradox módon minél több civilizációs vívmány jelent meg, minél kevésbé kellett tartani dögvésztől, jégveréstől, árvíztől, annál inkább előtérbe kerültek azok a bizonytalanságok, amelyeket maguk az emberek állítottak elő, csapdát állítva önmaguknak és az utánuk következőknek.

Az ember új ellensége: az ember

E társadalmi csapdáknak látszólag az információhiányos „korlátozott racionalitás” az oka, amely a résztvevőket megakadályozza abban, hogy végzetes következményekkel járó döntéseik kialakításakor figyelembe vegyék az összes lehetséges információt, amelyek birtokában megtalálhatnák az optimális megoldást. Valójában, mint arra Hankiss Elemér¹ rámutat, korántsem csak az információ hiánya idézi elő a csapdahelyzeteket, amelyek eredményeként visszajára fordul a Teremtő parancsának teljesítése. Hankiss a nyolcvanas évek elején így fogalmazott: kipusztulnak a tengerből a halak, elfogy a Föld belsejéből a nyersanyag és az energiaforrás, eltűnnek a tiszta vizek, elfogy az atmoszférából belelegezhető tiszta levegő. Keményen összegezve: megjelenik az ember új ellensége, aki nem más, mint maga az ember.

A társadalmi létől sosem volt idegen a szervezett felelőtlen-ség állapota. Ennek lényege, hogy a korrekciót lehetővé tevő információk meg sem születnek, vagy ha megszületnek, nem érik el a döntéshozókat, vagy ha éppen célba érnek is az információk, a döntéshozók képtelenek az információk adekvát feldolgozására. Visszacsatolás hiányában mire az emberek észreveszik a maguk által felállított csapdát, már nem tudnak kikeveredni belőle.

A gyors és széles körű információterjedés elvileg lehetőséget adna a csapdából való kikeveredésre, feltéve, hogy a sikeres

kommunikációt nem akadályozná az ellentétes érdekekben gyökerező korlátozott racionalitás.

A civilizációs folyamat globális elterjedése a Föld egyes társadalmi között minden korábbi mértéket meghaladóan szoros kapcsolatrendszeret teremtett, ami az egyes társadalmakat korábban kínzó bizonytalanságok egymásra hatását, és ezen keresztül megsokszorozódását idézte elő. A bizonytalanság egyetlen bizonyossága a válság, ami a maga előre láthatatlanságában globális szorongás és illuzionizmus táptalajává vált, hiszen bárhol, bármikor lecsaphat a Földön.

A világ elveszett biztonságának nyomába szegődve Ulrich Beck² a világ egészének biztonságát veszélyeztető kockázatok egész katalógusát adja. E veszélyeknek a korábbi veszélyekhez képest megkülönböztető sajátossága, hogy a Földön mindenütt jelen vannak, nincs hova menekülnünk előlük (leszámítva a más bolygókra való távozást). Beck szerint kiszámíthatatlan, hogy hol és mikor jelennek meg a veszélyek, amelyek katasztrofális hatásai ráadásul visszafordíthatatlanok és kompenzálhatatlanok. Tragikus, hogy minden esetben az ember maga a veszély előidézője, s egyben az ember az áldozat is. Rövid távon talán elkülönül a két szerep. Vannak, akik jól járnak, s vannak, akik rosszul. Hosszabb távon azonban, a következő generációk életében, elhomályosulhat a különbség, s az egykori elkövető ivadéakai éppúgy áldozattá lesznek, mint ahogyan áldozatokká válnak az áldozatok leszármazottai.

Az egész emberiséget fenyegető, ember teremtette veszélyek listáját áttekintve kézenfekvő elsőként a nukleáris energiára gondolni, amely iszonyatos mértékű pusztító erejét a XX. században háborúban és békében egyaránt megmutatta. Ám sem Hiroshima, sem Csernobil nem volt elég ahhoz, hogy az emberiség ki-verekezhessen magát a nukleáris energia létrehozásának csapdájából, és emiatt senki nem érezheti magát biztonságban a Földön, éljen bármelyik távoli zugban.

A légkör felmelegedése vitatott veszély, de számos jel van, amelyet nehezen lehet másként értelmezni, mint a környezet minőségének romlásaként. A modern társadalmi működés vele-

járájaként jelentkező negatív környezeti hatások szemmel láthatóan nem kímélik a Föld egyetlen pontját sem, s hatásaik egymást kölcsönösen felerősítve az egész emberiség jólétét fenyegetik, elvonva és ritkítva a túléléshez szükséges legalapvetőbb anyagokat (vizet, levegőt).

A fizikai szennyeződés okozta környezeti ártalmakhoz társulnak a genetikailag módosított élelmiszernövények tömeges termelése következtében jelentkező hatások, amelyek ugyancsak vitatottak, de elterjedésük semmiképpen sem kockázatmentes.

Az ember mint név mindeddig nem volt képes univerzális csoportképző, szolidaritási kategóriaként beépülni az identitásba, és emiatt nem túlzás az emberiség történelmét az emberek közötti harcok és öldöklések soraként láttatni, amelynek szakaszai csak abban különböznek, hogy egységnyi idő alatt, egységnyi területen mekkora számban irtottak ki embereket. Niall Ferguson³ nemrég megjelent műve meggyőzően érvel amellett, hogy a XX. század ezen a gyászos területen minden korábbi időszakot felülmúlt. A hagyományos módon megvívott háborúkat újfajta háborúk váltják föl, amelyek nem ismerik a békét. Permanens és globális fenyegetésként nyomasztja a civilizált világot a terrorizmus, amely mindenütt lecsaphat. A terrorfenyegetés pusztá lehetősége legalább olyan pusztító hatású, mint maga a megvalósult terrorcselekmény.

A posztmodern kapitalizmus játékszabályai messze elrugaszkodtak az Adam Smith⁴ által leírt rendtől. A „láthatatlan kéz” a világ pénz- és kötvénypiacán képtelen biztosítani az egyensúlyt a kereslet és a kínálat között, mivel egyik mögött sincs gazdasági realitás. A világ gazdasága egyre inkább piramisjátéokra emlékeztet, amelynek vége nem lehet más, mint az összeomlás. A „közlegelők tragédiája” Hankiss Elemér által leírt paradigmája szerint a globális piramisjáték minden résztvevője azt reméli, hogy éppen ő lesz az, aki megússza, ám ez a remény hiú ábránd marad.

Beck listájával szemben persze felhozható, hogy egyik esetben sincs szó végzettszerű determinációról, csak lehetőségekről, amelyek valószínűsége éppen az embereken múlik, akik megfelelő tudás, informáltság és kommunikációs eszköztár birtokában

minimalizálhatják a kockázatokat. Jobb, ha tudjuk, hogy mitől félhetünk, mint ha Voltaire Pangloss doktorának mintájára abban bizakodunk, hogy a lehetséges világok legjobbjában élünk.⁵

A rossz új tere

Az új infokommunikációs technológiák (IKT) megjelenése, rohamos terjedése, megállíthatatlan fejlődése teljesen átformálta a társadalmi, a közösségi és az egyéni élet terét. Ebben a térben mindenki világa mindenki más világával találkozik, akár akarja, akár nem. A mindenütt elérhető szélessávú internet a megfelelő kommunikációs eszközhez való hozzáférés és megfelelő használati készség esetén mindenkit összeköt mindenkivel. A világban élő embereket és közösségeiket egyetlen nagy, minden kontinenst átfogó kommunikációs hálózat kapcsolja össze. A hálózat nem teljes, vannak benne fehér foltok itthon éppúgy, mint a világ más tájain, de a foltok egyre zsugorodnak. Vannak tehát, akik még nem részesei ennek a globális rendszernek. Ez a hálózat jelen időben rendkívül gyorsan, rendkívül sok információ továbbítását teszi lehetővé, miközben semmi sem vesz el, mindennek nyoma marad, vagy éppen technikai probléma miatt elvesz, de legalább annak marad nyoma, hogy elveszett.

A jelen egy szemvillanás alatt válik múlttá, amely nem múlik el, hiszen hozzáférhető, megismerhető, kikutatható. A hálózat ugyan egyenlő mértékben hozzáférhető mindenki számára, de a tényleges részvétel mentén egyenlőtlenségek jönnek létre, amelyekről ma még nem tudható, hogy növelik vagy csökkentik-e a korábbi ismert, hatalmas feszítőerőt képviselő társadalmi egyenlőtlenségeket. De tudnunk kell: a pusztán fizikai hozzáférés önmagában kevés, hiszen megfelelő képzettség és tudás hiányában a technika és az ember között nem jön létre semmilyen tartalmi kapcsolat.

A társadalmi valóság korábban keletkezett konstrukciói az egyes kultúrák mércéi szerint meghatározták, hogy mi a jó és mi a rossz. Az IKT megjelenése révén megszületett a jó és a rossz új tere.

A következőkben a rossz új terében jelentkező jelenségekről írunk, amelyek pusztító ereje a korábbi ismert rosszal szövettségben megsokszorozódhat, és ezáltal jelentősen megemelkedik az emberi világ globális kockázati szintje.

Felvethető természetesen: miért a rosszról, s miért nem a jóról szól ez az írás? Ennek oka az, hogy meggyőződésünk szerint a jó csak akkor töltheti be szerepét az életben, ha legyőzi a rosszat. A jó győzelmének előfeltétele a rossz megismerése.

Technológiai veszélyek

Elsőként az IKT megjelenése révén jelentkező technológiai kockázatokról írunk. Az új infokommunikációs technológia fizikai szerveződésében súlyos veszélyek forrása, hiszen minden elemében emberi mű, amely felettébb sérülékeny, érzékeny és sebezhető. Fizikailag féltünk mindent, ami az új infokommunikációs technológia részét képezi, s félelmünk nem alaptalan, hiszen eszközeink sérülhetnek, elveszhetnek, az adathordozók „megsüketülhetnek” és „megvakulhatnak”, hálózataink elpusztulhatnak. Az IKT technológiai kártyavára bármely pillanatban összeomolhat. Ebben nincs különbség az előző korokhoz képest – amikor leégett az alexandriai könyvtár, amikor a háborúkban festmények, szobrok pusztultak el –, még ha az információs korszak elején az volt is az általános meggyőződés, hogy minden véglegesen megőrizhető. A megőrzés esélye azonban minden korábbi korszakhoz képest nagyobb, hiszen párhuzamos technológiákkal megoldható a „túlbiztosítás”.

A hálózatosodással az információk technológiai veszélyeztetettsége tovább nőtt, hiszen a szoftverek és adatbázisok lokális zavarai által okozott negatív hatások a rendszer bármely más pontjára rendkívül könnyen áttételeződhetnek. Vírusok, trójai programok, programférgek, kémprogramok,⁶ keyloggerek,⁷ zombihálózatok (pl. botnet),⁸ távoli eljárás hívás kezdeményezések⁹ zavarhatják az infrastruktúra rendeltetésszerű használatát. A fizikai térbe ártó szándékkal hatoló bűnözőkkel összehasonlítva a virtuális térbe beha-

toló bűnözők nagyságrendekkel nagyobb károkat képesek okozni (adat- és identitáslopás, port-, illetve IP- [Internet Protocol] átirányítások). A veszély attól oly nagy, hogy kevéssé vagyunk felkészülve rá, észrevétlenül terjed, s amikor már jelen van, késő.

Ami az IKT fizikai infrastruktúrája által létrehozott virtuális térbe bekerül, az mind adat. Kézenfekvő, hogy az adat van a legnagyobb veszélyben. Az adatok egyszer s mindenkorra eltűnhetnek, megváltozhatnak. Ez a veszély kivédhető lenne, de mindig lesznek olyanok, akiknek éppen a törlés, a változtatás, a hamisítás a szándékuk. A behatolók célja lehet az adatok ellopása, illetéktelen felhasználása, az adatokkal való visszaélés.

Az adatvesztés, adatmódosulás és adatromlás veszélyeinek forrásai a terminálok, központi és lokális szerverek, valamint az adathordozók. Az igazán fontos adatokat hálózaton nem elérhető nagy adatbázisokon tárolják, egyszerre több helyen is, ami garanciát adhat az adatok biztonságáért aggódók számára.

A hétköznapi felhasználók számára riasztó, hogy a szüntelen protokollváltozások az egymást követő IKT-generációk közötti kommunikációt veszélyeztetik, a később megjelenő technológiák használói számára hozzáférhetetlenné téve a korábbi eszközök által létrehozott adatállományt. Eltűnnek a családi fotók, nem maradnak meg az információk esetleg egy-egy technológiaváltással. Régen a családfők a családi Biblia utolsó oldalára rögzítették, mintegy palackpostaként, a ritka pillanatok képeit a későbbi nemzedékek számára.

Veszélyben vannak az adattovábbító hálózatok, amelyek fizikailag megsemmisülhetnek, túlterhelés esetén lefagyhatnak, használatképtelenné válhatnak. A hálózatok legnagyobb előnyei egyben a legnagyobb hátrányok forrásai is. Mivel a hálózatok egymás erőforrásaira épülnek, ezért egy nagyobb kiterjedésű hálózati hiba esetén dominóeffektus jöhet létre, amelynek során bizonyos eszközök, szerverek időszakosan működésképtelenné válnak, ami – lehetetlenné téve a szolgáltatásokat – láncreakciót eredményez. A hálózati működési nehézségeket nemcsak az ártó szándékú logikai támadások okozhatják. A hálózat tervezése,

méretezése, programozása is veszélyforrás. Különösen komoly nehézségek forrása, és valós probléma, ha a tervezők rosszul mérik fel a felhasználók számának növekedési ütemét. A híd is leszakad, ha rosszul számították ki teherbíró képességét.

Informatikai bűnözés

Az adatok és a hálózat léte kitermelte az informatikai bűnözést, amelyből három típust különböztetünk meg (a részleteket lásd Rácz Bencze fejezetében is).

Az első az illetéktelen behatolás, a hardver elleni támadás: ide tartozik a jogosulatlan belépés, a gépidőlopás és a mikrochipek jogtalan másolása.

A második a szoftver elleni támadás. Tipikus példa erre a programmanipuláció és a szoftverlopás.

A harmadik típusú támadás az adat ellen irányul, amelynek során a támadó ellopja az adatot, megghamisítja az adatbázist, visszaél az adatokkal, felmérhetetlen károkat okozva az adatok tulajdonosainak (részletesen lásd kötetünkben Szabó Endre és Rácz Bencze írásait).

A virtuális tér éppúgy lehetőséget nyújt a lopásra, csalásra, kémkedésre, szabotázsra és zavarkeltésre, mint a fizikai tér. Az elkövetők technológiai lépéselőnyben vannak a felhasználókkal szemben, akik sok esetben egyáltalán nincsenek tudatában az adataikra (és ezáltal rájuk) leselkedő veszélyeknek, amelyek hatásai éppen olyan pusztítók, mint a fizikai térben rájuk leselkedő veszélyek (lásd még Szabó Endre és Rácz Bencze fejezetét).

Társadalmi veszélyek

Az adat tere virtuális ugyan, de az adatok létrehozói, hordozói, használói a társadalom valóságos terében működő aktorok és szervezetek. A társadalom életébe beágyazódott IKT zavarai komoly

társadalmi zavarokat okozhatnak; gondoljunk csak egy repülés-irányítói rendszer meghibásodására, vagy a banki rendszer akár csak párórás leállására. Az IKT virtuális teret hoz léte, amely új, másutt ismeretlen bűncselekmények táptalaja. Az internet bűnözőit ez a táptalaj elteti. Az információlopás, a bankkártyákkal való visszaélés, a hamis weboldalak elhelyezése a ma még csak születő-félben lévő kiberkriminológia vizsgálódásának lehet tárgya. (Lásd erről részletesebben Szabó Endre és Rácz Bencze fejezetét.)

A web 2.0 logikája által létrejött „társadalmi média” alulról építkezik, s annál hatékonyabb mind a gazdaságban, mind a politikában, minél többen vesznek részt benne. Ugyanakkor ez az előny hátrány is lehet, hiszen a mozgósítás célja kártékony is lehet. A világhálón könnyűszerrel el lehet helyezni csoportközi gyűlöletet keltő tartalmakat, gyermekek jogainak sérelmével létrehozott pornográf képeket és egyéb jogellenes adatállományokat. Nincs eszköz, amely lehetővé tenné a hatékony védelmet (lásd még Z. Karvalits László és Vajda Zsuzsanna kötetünkben megjelent írásait.)

Nem túl hatékony a társadalom védekezése a világhálóra került programok és tartalmak szerzői jogainak megsértőivel szemben (másolás, forgalmazás, tiltott kereskedelem). A piaci eszközök ma még inadekvátak. Várnunk kell az új piaci modellekre, amelyek képesek lesznek a ma még áthidalhatatlannak tűnő érdekellentétek áthidalására a tartalmak jogtulajdonosai és fogyasztói között.

Az internethasználók társadalma nincs tudatában a totális megfigyelhetőség veszélyének. Az IKT technológiája komoly segítség azok számára, akiknek célja a személyes, a különleges adatok, a jogilag védett titkok kifürkészése, illetéktelenek számára való hozzáférhetővé tétele, az elektronikus postán küldött levelek illegális elolvasása, tárolása (lásd még Székely Iván fejezetét).

Illúziónak bizonyult az a várakozás, miszerint a web 2.0 alapú „társadalmi média” a társadalmi nyilvánosság új, minden korábbihoz képest demokratikusabb és szabadabb fórumáját nyitja meg. A web 2.0 által teremtett kommunikációs lehetőségek teré-

be betóduló tömegek hiú, önközpontú, rövid, efemer érvényű közlései távolról sem a megfontoltság és a racionális eszmecsere példái lettek. A társadalmi média a tömegek várt bölcsessége helyett a tömegek ostobaságának lett színtere (részletesen lásd Z. Karvalics László írását kötetünkben). Az új kommunikációs technológia megjelenése ugyanis nem változtatott a technológia használoinak sokaságára érvényes kognitív egyenlőtlenség törvényén, amely a Gauss-görbe¹⁰ kegyetlenségével szűkre szabja a valóban tehetségesek körét, akik törpe kisebbséget alkotnak a gondolkodni restek¹¹ többségével szemben.

Az internethasználat elterjedése egyenlőtlenül ment végbe a társadalomban. Digitális szakadék jött létre, amelynek egyik oldalán az internethasználók, másik oldalán az internethasználat-tól tartózkodók vannak. Az internethasználat egyáltalán nem csökkentette a korábbi társadalmi egyenlőtlenségeket, mint ahogy arra sokan számítottak, hanem rájuk épülve tovább fokozta az egyenlőtlenségeket. Európa internethasználati térképére tekintve az is kiderült, hogy Nyugat- és Észak-Európa történelmi előnyei a napi internethasználók egyes országokban talált arányaival tökéletesen korrelálnak.

Az elsődleges digitális egyenlőtlenségek csökkenése egyáltalán nem jelenti azt, hogy ne alakuljanak ki másodlagos digitális egyenlőtlenségek, amelyeket az IKT-technológia elképesztően gyors fejlődése okoz. A Rogers-törvény¹² minden egyes IKT-újítás megjelenése esetén életbe lép, megkülönböztetve az innovátorokat, a korai alkalmazókat, a korai és a későbbi többséget, valamint az adott innovációt alkalmazni képtelen lemaradókat. Ily módon az információs társadalom közönsége újra meg újra strukturálódik, ahányszor csak megjelenik egy új „killer application”¹³ vagy egy új hardvereszköz. Mindig lesznek netokraták,¹⁴ netizenek¹⁵ és „netproletárok”. Ha a gazdasági és szimbolikus javak optimálisan oszlanak is el a társadalomban, az életkor mindig meg fogja határozni, hogy kik lesznek az élenjárók, és kik a lemaradók. A fiatalok előnye a technológiai innovációk elsajátításában behozhatatlan az idősebbekhez képest, akiknek, ha akarják,

ha nem, az életkor növekedésével kopik az érzékenységük az új és szokatlan (ráadásul részben valóban szükségtelen) technológiai megoldásokkal szemben. Mindez sosem az egyénre, mindig a tendenciára igaz.

Kulturális veszélyek

A kultúrára leselkedő veszélyeket ítélem a legsúlyosabbnak. Maga a technológia csábít az öncélú újításokra, amelyek egyik része alkalmazásra hajlandó innovátorok hiányában elhal, másik része ideig-óráig megmarad, míg ki nem derül, hogy van helyette újabb vagy jobb. Az IKT fejlesztői a fejlesztések során sokszor nem veszik figyelembe a legalapvetőbb humán szempontokat sem, kísérleti alanyként kezelik a társadalmat, ami létrehozza a „fölöslegesség kultúráját”, megállíthatatlanul termelve a környezetre ártalmas szemetet. Másfelől a fejlesztések leállíthatatlanok, hiszen az IKT lényege a váltás, még akkor is, ha a későbbi nem feltétlenül jobb, mint az előbbi. Ma még felelőtlenség lenne bármit is állítani arról, hogy mit tartanak majd kultúrának a kibertér látogatói, és mit nem. Annyi bizonyosnak tűnik, hogy az internet előtti kultúra kibertérbe vezető útja nem lesz könnyű.

A Nemzeti Kulturális Alap megrendelésére a Szonda-Ipsos Véleménykutató Zrt. által 2008 végén a magyar felnőtt népesség háromezer fős országos reprezentatív mintáján végzett vizsgálat kapcsán azt találtuk, hogy a minta majdnem fele a televíziónézést leszámítva (49%), semmilyen kulturális viselkedést nem tanúsít. Ennek a csoportnak a tagjait neveztük kulturális szegényeknek. Legkevesebben a kulturális gazdagok voltak (11%), akik azért kapták ezt a besorolást, mert nem válogatnak a kulturális viselkedések fajtái között, s mindenféle kulturális eseményen (színház, koncert, kiállítás, fesztivál stb.) részt vesznek, ha van idejük, kedvük, pénzük, továbbá könyveket is olvasnak. A mintába került személyek 20%-a volt nevezhető a magas kultúra közönségének, amelynek tagjai tevélegesen érdeklődnek az irodalom és a kép-

zőművészet, valamint az előadói művészetek iránt. Hasonló arányt ért el (19%) a tömegkultúra közönsége, amelynek tagjai a népszerű kulturális események résztvevői, látogatói a plázákban található kulturális színtereket, könnyűzenei koncerteket, sporteseményeket stb.

Az internetezés léte vagy hiánya szignifikáns összefüggést mutatott a kulturális viselkedés típusai szerint képzett csoportokkal. A kulturális szegények 80%-a nem internetezik, ami arra utal, hogy akik nem interneteznek, azok egyben igen nagy valószínűséggel kulturális szegények is. Fordított a helyzet a kulturális gazdagok körében, akiknek 86%-a internetező. Kisebb arányú, de még mindig domináns az internetezők jelenléte a tömegkultúra és a magas kultúra közönségében. Ugyanakkor azt tapasztaltuk, hogy a magas kultúra közönsége jelentős arányban (45%) van jelen a nem internetezők között is. A felmérés adatait tartalmazza az 1. táblázat.

	Nem internetezik	Internetezik	Összesen
Kulturális gazdagok	14%	86%	100%
Kulturális szegények	80%	20%	100%
Tömegkultúra-közönség	30%	70%	100%
Magaskultúra-közönség	45%	55%	100%

1. táblázat. Kulturális viselkedéscsoportok és internetezés
Khi-négyzet érték: 777,96 df: 3 szig. 0,000 Cramer's V: 0,51

A kultúrát tehát nem kell féltetni az internettől, amennyiben az internethasználóknak van elég kulturális tőkájük (műveltségük, ismeretanyaguk, közvetlen kulturális élményük) ahhoz, hogy meg tudják találni a kultúra szövevényét az internetben. A kultúra azok életében nincs jelen ténylegesen, akiknek az életéből az internet is hiányzik. Az internetezéstől való tartózkodás azonban nem feltétlenül jár együtt a kulturális elszegényedéssel. Az internet azoknak ad, akiknek már van kulturális tőkájük.

Az említett vizsgálat eredményei szerint a kulturális piac potenciális résztvevői többen vannak, mint amit a tényleges kulturális fogyasztás adatai sejtetnek. A vizsgálat azt mutatta, hogy amennyiben a válaszadó életvezetését autonómia jellemzi, és internethasználathoz jut, akkor nagy az esélye annak, hogy tagja lesz a kulturális közönség valamelyik szegmensének.

A szociológiai vizsgálatok eredményei szerint a digitális bennszülöttek¹⁶ generációi teljesen másként viszonyulnak a kultúrához, mint a digitális bevándorlók, vagy azok, akik nem tartoznak az információs társadalomhoz. A digitális bennszülöttek a fiatalok, akik beleszülettek abba a környezetbe, amit a mobiltelefon, a PC, a laptop, a digitális kamera és a naponta elérhető internethasználat jelent. A digitális bevándorlók ezzel szemben már felnőttként, korai szocializációs tapasztalatok hiányában találkoztak az infokommunikációs technológiával, amelynek eszközei és lehetőségei kezdetben idegenek voltak számukra.

A digitális bennszülöttek internethasználata teljesen más, mint a digitális bevándorlóké. A digitális bennszülöttek igen aktívak a „társadalmi média” használatában, köztük sokkal több a „prosumer”, aki nemcsak fogyasztja, hanem termeli is a tartalmat.

Nem várható, hogy az információs korszakban változatlan módon megmaradnak az információs korszak előtt keletkezett kulturális értékek, kulturális viselkedések és kulturális intézmények. Hihetőnek tűnik a fenyegető jóslat, miszerint a Gutenberg-galaxis eltűnik, és magával visz sok mindent, amit e galaxis lakói értékesnek gondolnak. A mindenütt jelen levő, mindenki számára elérhető és mindenki számára szereplési lehetőséget kínáló internet sikermutatója az elérték száma. Minél többen néznek, hallgatnak valamit, annál inkább ráirányul a közfigyelem. A siker azonban pillanatnyi, hiszen a közfigyelemért folytatott verseny kíméletlen. A „figyelemgazdaság” egyre újabb és újabb ingereket követel, amelyek akkor aratnak sikert, ha egyszerűek, és érzelmekre vagy előítéletekre épülnek. A web 2.0 ugyan lehetőséget ad arra, hogy érdeklődési körök mentén közösségek jöjjenek lét-

re, de az egyes körök egymásra hatása szerfelett korlátozott, s a látogatottságon kívül nincs mérce, amelynek alkalmazása révén megmondhatnánk, hogy mi az értékes és mi nem az az internet-re került tartalmak óceánjában (lásd még Talyigás Judit Felvezetésében).

Pszichológiai veszélyek

A görög mitológia mindentudó tengeristenét, Próteuszt Poszeidón, a tengerek királya felruházta azzal a hatalommal, hogy tetzése szerint változtassa alakját. Az internet kommunikációs térében mindenki Próteusz lehet. Az identitás változtathatósága a virtuális térben ellehetetleníti az interperszonális találkozások fizikai térben működő visszacsatolási funkcióit. Az elszabadult ént semmi és senki nem korlátozza vágyai megvalósításában, amihez készséges partnereket talál, akik hasonló módon tetszésük szerint változtatják alakjukat. Az internet társas közege az illúziók és a valóságos életben ki nem élt fantáziák táptalajává válik. A valóság virtualizálódik, miközben a virtuális valódinak tűnik. Mindez kísértetiesen emlékeztet Gulácsy Lajos Nakonxipánjára,¹⁷ amelynek lakói nem tudnak és nem is akarnak visszamenni a való életbe.

Az internet révén szerzett társas élmények okozta öröm ára az internettől való függés (részletesebben lásd a kötetben Demetrovics Zsolt írását). Csupán klinikai és kriminológiai tapasztalatok bizonyíthatják, mekkora a veszélye annak, hogy a virtuális térben felszabadult és elszabadult én egyre inkább kiszorul a valóságos társas térből, könnyű prédájává válva azoknak, akik ki nem elégített vágyai, szenvedélyei kiszolgálására vállalkoznak.

Az IKT-eszközök fejlesztése egyre inkább afelé halad, hogy az ember szükségképpen tökéletlenségekkel teli kognitív funkciói kívül kerüljenek a lélek terein. A GPS szükségtelenül teszi a térben való tájékozódás képességét. A Google átveszi az emlékezet funkcióját. Az internetes játékok kiváltják a fantáziát. A döntéstámogató szoftverek leveszik a felelősség terhet az emberről.

Ma még nincsenek olyan gépek, amelyek átmennének a Turing-teszten.¹⁸ Az emberek értetlensége miatt tragikus sorsú brit matematikus a gépek értetlenségének próbájaként írta le a róla elnevezett tesztet. Turing azt állította, hogy egy gép akkor értelmes, ha egy ember öt-hat percig képes kommunikálni vele anélkül, hogy rájönne, géppel van dolga. Nem tűnik túl merész jóslatnak, ha leírjuk: közeleg az idő, amikor a „dolgozók internete” és az emberek internete között elmosódik a határ, s megjelennek az intelligens gépek, amelyek bizonyos funkciók ellátása során nem lesznek megkülönböztethetők az emberektől.

A kognitív terhek viselése alól felmentett emberben óhatatlanul felszabadulnak az érzelmek, amelyek átélésére és kommunikációjára a gépek sosem lesznek képesek. A kontroll nélkül maradt érzelmek a paroxizmus¹⁹ és a barbarizmus szélsőségei között ingadozva felerősítik a tudattalan hatásait az emberben. Az internet anonim közösségi terében az ember a másik embernek természetesen nemcsak farkasa, hanem pásztora is lehet. Ez esetben a „nem mondhatom el senkinek, elmondom hát mindenkinek” maxima működik, aminek révén önszegítő csoportok jöhetnek létre (bár e csoportoknak nagyon kell tudniuk védekezni a soraikba befurakodó, báránybőrbe bújt farkasok ellen).

Az IKT-eszközök fejlődése és tökéletesedése sokakban már ma is szorongást kelt. A technofóbia „splendid isolation”-re²⁰ ítéli a szorongót, akinek identitása része lesz minden technológiai újítás elítélése, aminek bázisán új ludditizmus²¹ bontakozhat ki.

Ellenszerek

Az új ludditák kudarcra vannak ítélve. A civilizációs haladást nem lehet visszafordítani. Az IKT-eszközök megjelenésének, terjedésének nincs alternatívája a társadalomban. A jelenlegi, veszélyekkel teli helyzetnek viszont van alternatívája.

Az internet veszélyei ellen való védekezés közfeladat. Szét kell szaggatni a tudatlanság fátylát, amely még azok látását is elho-

mályosítja, akik benne élnek az információs társadalomban. Az információs társadalmon kívül állók esetében a tudatlanságot súlyosbítják az előítéletek, félelmek, gátlások. Mint minden eszköz, az IKT használata esetében is kulcsényező a tudatosság. Mivel az IKT változása és fejlődése megállíthatatlan és folyamatos, ennek megfelelően a tudatosságot biztosító képzésnek is folyamatosnak és folytonosan megújulónak kell lennie.

A tudatosság legfontosabb eleme a tudás, az ismeret és a képesség a biztonság feltételeinek megteremtésére. A veszélyek egy része ezáltal elhárítható. A veszélyek másik része a tudatosság szintjének emelése által nem hárítható el, de a veszélyek hatása mindenképpen kevésbé pusztító, ha felkészülünk fogadásukra.

Közpolitikai feladat a képzés és a tájékoztatás megteremtése és karbantartása, amelynek révén mindenki, aki az IKT-val kapcsolatba kerül, megállapíthatja, megértheti, hogy mi a jó és mi a rossz a virtuális térben, mikor jár tilosban és mikor szabad a pálya. Közfeladat a szabályozás kidolgozása az internet elérését lehetővé tevő infrastruktúrára éppúgy, mint az elérhető tartalmakra és szolgáltatásokra, beleértve az internetre lépők jogainak és kötelességeinek szabályozását. A jövő internete nem lehet monopóliumok prédája, de nem lehet az anarchia színtere sem. Az európai uniós és tagállami szabályozás nem oldhat meg mindent. Ezért fontos lenne, ha az IKT-kör érdekelt vállalatai szakmai szegmensenként létrehoznák a maguk etikai kódexét, amelynek rendelkezéseit nem a törvény, hanem a tisztesség szankcionálná, még ha tudjuk is, hogy a jó és a rossz közötti határok óhatatlanul *fuzzy*²² jellegűek.

Ez persze csak a végeredmény. Ami közfeladat, az a képzés és az önszabályozás szükségének tudatosítása.

Az internet veszélyei ellen leginkább az interneten lehet küzdeni. Közfeladat, hogy az interneten elérhetőek legyenek a felhasználói tudatosságot szolgáló tartalmak, működjön az azonnali bevetésre kész hálózati rendőrség, rendelkezésre álljanak és rendszeresen frissüljenek a biztonságot szolgáló szoftverek.

Nagyon sokat segíthet, ugyanakkor árthat is a média. A napi internethasználók arányát tekintve Magyarország nem állna az

európai országok rangsorában az utolsók között, ha az elmúlt években a média közpolitikai jelentőségéhez mért komolysággal és súllyal foglalkozott volna az információs társadalom ügyével. Az információs társadalom médiareprezentációja Magyarországon sajátosan kétarcú. A napilapok elkülönített mellékleteiben szakmailag magas színvonalú írásokkal találkozik az információs társadalom iránt eleve elkötelezett olvasó. Ugyanazon napilap napi információs oldalain viszont a „Szabó Brigitta”²³ szoftver által létrehozott ellenséges, értetlen, téves értesüléseken alapuló írások jelennek meg, amelyeket a magas színvonalú szakmellékletet átlapozó olvasók olvasnak. Ugyanez a helyzet a heti- és havilapok esetében. Vannak kiváló szaklapok, amelyek olvasói zárt kört alkotnak, akiket összeköt a háttértudás és a szakzsargon ismeretének közössége. A nem szakmai közönséget célzó lapok csak akkor adnak hírt az információs társadalom ügyeiről, ha azok kétes értékű szenzációkat hordoznak. Hiányoznak az élet e-minőségét testközelbe hozó, a legjobb gyakorlatokra koncentráló, közérthető írások és tartalmak.

Az internet könyvünkben felsorolt (s fel nem sorolt) veszélyeivel szemben a társadalom akkor védekezhet a leghatékonyabban, ha valamennyi érdekelt folyamatosan kapcsolatot tart egymással. A védelem csak akkor lesz eredményes, ha összefognak a civil szervezetek, az iskolák, a hatóságok, az akadémiai és egyetemi kutatóintézetek, valamint az üzleti vállalkozások annak érdekében, hogy legyenek olyan népszerű programok és akciók, amelyek segítségével mindenki, aki az internettel érintkezésbe kerül, megvédheti magát, szeretteit és értékeit.

Szabó Endre Győző *Jogász, adatvédelmi szakértő, a Közigazgatási és Igazságügyi Minisztérium főosztályvezető-helyettese az Igazságügyi Együttműködési és Nemzetközi Magánjogi Főosztályon*

A SZEMÉLYES ADATOK VÉDELMÉNEK KÉRDÉSEI A VIRTUÁLIS VILÁGBAN

A személyes adatok¹ védelméhez fűződő jogot legmagasabb szintű jogforrásunk, az Alkotmány rögzíti. A jog tartalmát az Alkotmánybíróság információs önrendelkezési jogként határozta meg. Döntései során úgy tekint e jogra, mint amelynek alapján nem csak az illeti meg a polgárt, hogy adatai és ezeken keresztül ő maga védelemben részesüljön, hanem mindenkinek joga van saját személyes adataival rendelkezni. Más nem jogosult erre helyette, kivéve az Országgyűlést, amikor olyan törvényt hoz, amely a személyes adatok kötelező szolgáltatását valamely konkrét esetben előírja. Ez érthető, mert az állam működése során számos adatra van szükség, az adóigazgatástól kezdve az egészségügyi szolgáltatásokon át a nyugdíjak megállapításáig és folyósításáig, amelyek ezen adatokon is alapszanak. Ezekben az esetekben nem lehet az egyén, azaz az adatalany döntésétől függővé tenni az adatok szolgáltatását: azok kezelését nyilvánvalóan kötelezővé kell tenni.

Minden olyan esetben, amikor az Országgyűlés nem szabályozta és nem rendelkezett a személyes adatok kötelező kezeléséről, az információs önrendelkezési jog érvényesül: azaz az egyén az egyedi jogosult az adatok, az adatai(!) sorsáról dönteni.

A következőkben személyes adataink kezeléséről és védelméről gondolkodunk a virtuális világ sajátosságait figyelembe véve. A későbbiekben megcáfolandó kiindulópont szerint a virtuális világ megpróbálja leképezni a való életet, és a való életben végrehajtható műveleteinket egy lényegesen könnyebben kezelhető közegbe viszi. Nem történik tehát más, mint hogy a való élet megkettőződik ott, ahol erre szükség, illetve lehetőség van.

Társadalmi életünkben (a való életben) számos különféle viszony alakul ki közöttünk és más szereplők között. E kapcsolatok egy része kívül esik a jog érdeklődési területén, és nem szabályozza azokat. Ilyen például a barátság. Másik részét azonban a jog – hol pontosabban, hol inkább megengedő jelleggel – szabályozza. Ezeket a jogilag szabályozott viszonyokat nevezzük jogviszonynak. A jogviszonynak lehet két szereplője, ilyen például a házasság, de lehet sok szereplője is. Érdekességgént említhetjük a környezet védelmét érintő ügyeket a hatásterületen élők nagy száma miatt. A jogviszony szereplője lehet természetes személy, gazdasági társaság, vagy éppen az állam valamely szerve is. A szereplők számától és jellegétől függetlenül a jog meghatározza a jogviszonyban szereplőket megillető jogokat és az őket terhelő kötelezettségeket. A jogviszony tartalma az egyes szereplők jogainak és kötelezettségeinek összessége. A későbbiekben az egyes élethelyzetek elemzését az említett fogalmak segítségével értelmezzük.

Adataink a való és a virtuális világban

– társadalmi viszonyaink jogi szabályozottsága

Melyek azok a társadalmi viszonyok, kapcsolatok, amelyek a virtuális világba könnyen átvihetők? Vegyünk egy egyszerű példát: ügyfelei vagyunk egy banknak, amely felkínálja számunkra a net-

bankolás lehetőségét. A megadott felhasználói név és jelszó (vagy adott alkalomra szólóan generált kód) birtokában a kockázatokhoz mértén megfelelően védett felületen tudjuk ügyeinket intézni a virtuális bankfiókban. Ilyen módon nyílik lehetőség például számláink befizetésére, vagy éppen arra, hogy átutalás révén kölcsönt adjunk valakinek. Az eredeti jogviszony alanyai, a jogok és kötelezettségek rendszere e virtuális közegben is azonosak a való életben fennállókkal (bank-ügyfél, kölcsönadó-kölcsönvevő stb.). A személyes adatok felhasználásával és védelmével kapcsolatban itt tehát annyit mondhatunk, hogy az eredeti jogviszonyhoz képest nincs változás. Az adatok biztonsága érvényesül, és az ügyfél is vigyáz a bejelentkezéshez szükséges adataira és eszközeire, további aggályunk adataink jogszerű kezelésével összefüggésben nem merül fel. A bankunkkal fennálló jogviszony folyamatos, függetlenül attól, hogy hányszor látogatunk el virtuálisan vagy személyesen is a bankfiókba.

A bank napi életünk észrevétlen, de örökös társa lett, hiszen a bankunkhoz fűződő kapcsolatunknak köszönhető, hogy termékek, szolgáltatások vásárlására nyílik lehetőségünk bankkártyával. Vegyünk egy konkrét példát: ha repülőjegyet vásárolunk, kapcsolatba kerülünk egy légitársasággal is. Ekkor háromszereplős jogviszony alakul ki, amelyet a jogszabályok, illetve a különböző szereplők közötti szerződések rögzítenek. Ezekben az esetekben a virtuális világ szereplői ugyanazok, mint akik a való életben is találkozónának, csupán az érintkezés módja és felülete más. Természetes, hogy a virtuális ügyletek létrejöttéhez és lebonyolításához szükség van az internetre, a fizetés biztosítását lehetővé tevő szolgáltatásra és szolgáltatóra. Ezek igénybevétele révén adatok generálódnak. Egyre több tehát a szereplő és az adat. Ez a többletként jelentkező adatigény eredeti céljainkkal – példánkban a repülőjegy-vásárlással – egy irányba mutat, így nem bomlik meg a jogviszony tartalmát képező jogok és kötelezettségek rendszere. Egyszerűbben fogalmazva: nem növekednek aggályaink a virtuális világba való kilépéssel.

Említhetjük még példaként az állami szervekkel való kapcsolattartásra szolgáló Ügyfélkaput. Ennek révén interneten keresz-

tül tudjuk állampolgári ügyeinket intézni, azaz kötelezettségeinket teljesíteni vagy jogainkat gyakorolni. Ekkor is változatlanok a jogviszony szereplői a való világhoz képest: állami vagy önkormányzati szervek és az állampolgár, az adózó. A jogok és kötelezettségek felépítése sem változik, tehát egy tiszta kivetítésről van szó, pusztán a kapcsolattartás módja más. Így az adatvédelmi jogi elemzés is elsősorban az azonosítás és az adatbiztonság kérdéseit vizsgálja e gyakorlat bevezetése során.

A személyes adatok felhasználásának korlátja: a célhoz kötöttség és az adatminimum elve – a személyes adatok mindennapi alkalmazásai

A magyar adatvédelmi törvény minden adatvédelmi tárgyú nemzetközi dokumentummal összhangban a jogszerű adatkezelés feltételévé teszi a célhoz kötöttség érvényesítését. Ezen alapelv szerint személyes adatot kezelni csak meghatározott célból, jog gyakorlása vagy kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak. A célhoz kötöttség azt írja elő, hogy a felhasználható adatok köre a jogviszony jellegéhez, tartalmához igazodik.

A személyes adatok felhasználásakor az adatkezelőnek – vagyis a jogviszony egyik szereplőjének – mindenkor tudnia kell igazolni, hogy mely adatot milyen jog gyakorlása vagy milyen kötelezettség teljesítése érdekében kezel. Ha ezt nem tudja igazolni, akkor adatkezelése kifogásolható. Ha olyan jogszabályra vagy kötelezettségre hivatkozik, amely nem illeszkedik a jogviszonyba, akkor az adatvédelmi jogi elemzés ahhoz vezet, hogy az adatkezelés nem felel meg a célhoz kötöttség elvének, vagyis az adatkezelés jogellenessé válik.

Nézzünk egy konkrét esetet. A banki példánál maradva: a banki ügyfél elektronikus postacímének rögzítése a kapcsolattartás céljából indokolható lehet, ezért azt a bank tárolhatja, ha ehhez az ügyfél hozzájárul. Attól azonban nem teheti függővé a bank az internetes bankolásra vonatkozó szerződés aláírását, hogy az ügyfél hozzájá-

rul-e a bank reklám célú üzeneteinek fogadásához. A személyre szóló marketingtevékenység ugyanis a magyar jog szerint önálló jogviszony, és a felek önkéntes együttműködésén, akaratán alapul. Ha tehát a bank csak akkor köt internetes bankolásra irányuló szerződést, ha az ügyfél hozzájárul ahhoz, hogy marketingüzeneteket küldjenek neki, akkor a bank a jog nyelvén szólva a célhoz kötöttség elvének sérelmével jár el, hiszen a két jogviszony (internetes bankolás és direktmarketing-tevékenység) egymástól elkülönítendő, jogi értelemben külön kezelendő. Így az ügyfél elektronikus postacíme az ügyfél eltérő rendelkezésének hiányában csak az internetes bankolással összefüggésben használható fel, más célra nem vehető igénybe. Mert az elektronikus postacím is személyes adat!

Hasonlóan fontos, hogy a jogalkotó az adatminimum elvét adatvédelmi törvényünk részévé tette. Eszerint csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, de csak a cél megvalósulásához szükséges mértékben és ideig. A cél a jogviszony – egy adott tevékenység – megvalósulása, amelyhez értelemszerűen szükség van személyes adatokra (a személyt azonosító adatokon² túl például a bankszámla számára). A jog ismét a jogviszonyt állítja a középpontba.

Olyan személyes adat tehát, amely a jogviszony szempontjából elengedhetetlen, jogszerűen kezelhető, de a jogviszony megvalósulásához elengedhetetlen adatok is csak addig kezelhetők, tárolhatók, ameddig azokra valóban szükség van.

Az elmondottakra jó példa, hogy az országgyűlési és önkormányzati választásokon jelöltként indulni kívánó személyek meghatározott számú ajánlószelvényt kötelesek leadni az illetékes választási szervnek. Ebben az esetben az ajánlásokra előírt határidő lejártával a jelölnél maradó (le nem adott) ajánlószelvényeken szereplő személyes adatok kezelése is okafogyottá válik, ezért a választási eljárásról szóló törvény a szelvények megsemmisítését írja elő. A jogi szabályozás azonban nem mindig szab konkrét határidőt az adatok törlésére, megsemmisítésére. Ha nincs egzakt szabály, akkor a célhoz kötöttség és az adatminimum elvéből ki-

indulva kell meghatározni a szükséges tárolási időtartamot. A le-adott szelvények megsemmisítésének idejét – a választást követően – már előírja a törvény, védve a választók adatait – pontosabban a választókat adataik más célú felhasználásának lehetőségétől.

Meddig terjed az egyén döntése saját adatai felhasználásáról?

Az információs önrendelkezési jogot, mint láttuk, kizárólag az Országgyűlés korlátozhatja, ha valamely területen a kötelező adatkezelésről törvényt alkot. A jog úgy tekint az érintettre, az ország lakosára (az adatok alanyára), mint aki saját adatai sorsának meghatározását illetően a legfelkészültebb. Nincs szüksége mások támogatására ebben a kérdésben, felnőtt emberként ő, és csak is ő hozhat döntést arról, hogy mások előtt feltár-e, és ha igen, milyen mélységben, vele összefüggésbe hozható adatokat.³ A jog tehát hagyja, hogy az adatok alanya az adatok későbbi felhasználásának körülményeit mérlegelje, és e mérlegeléstől függően döntson adatai kiszolgáltatásáról, használatuk engedélyezéséről. Ezt a döntést akkor tudja további aggályok nélkül meghozni, ha teljesülnek a tájékoztatásra és a tájékozódásra vonatkozó elvárások.

Felmerül a kérdés: mi történik akkor, ha az adatalany rosszul mérlegelt, és döntését utólag vissza szeretné vonni? Az adatvédelmi jog világos választ ad erre: az érintett kérheti, hogy az adatkezelő erre irányuló kérése esetén törölje (semmisítse meg) az érintettre vonatkozó adatokat. E jog nem illeti meg az adatalanyt, ha kötelező adatkezelésről van szó. Ez a kérdés jogi oldala. A gyakorlat – különösen a virtuális világban – ennél bonyolultabb. Az interneten elérhető adatok körében sajnálatos módon gyakran nem beszélhetünk az utólagos mérlegelés lehetőségéről. Az internet elméletileg az „örök nyilvánosság” közege. Bekerült adatainkat egyegy forrásból törölhetjük vagy töröltethetjük, másutt azonban megmaradhatnak. Az adattulajdonos csak abban reménykedhet, hogy a róla felkerült adatok nem keltik fel mások érdeklődését, és nem fognak azzal visszaélni.

Az érintett tehát teljes mértékben szabadságot élvez a személyes adatairól való rendelkezést illetően, kellő körületek nélkül azon-
ban e szabadság a virtuális világban és azon keresztül a való életben
utólag nehezen visszafordítható következményekkel járhat.

A közösségi oldalon megadott adataink és a célhoz kötöttség

A közösségi portálokon a profil létrehozásakor irányított módon
zajlik adataink megadása. A való életben a legritkább esetben sze-
repelnek az egyénre vonatkozó, általánosnak tűnő kérdések a ki-
töltésre váró rubrikák között, például a „beszédes” kedvenc film,
könyv és a többi. Ezek mellett a vallásra vonatkozó kérdés szinte
természetesnek tűnhet. Nem tiltja semmi, hogy egy ilyen közeg-
ben – a közösségi oldalon – a szolgáltató felkínálja a lehetőséget,
hogy a közösség tagjaival megosszuk a felekezeti hovatartozá-
sunkra vonatkozó adatot. De ezt a kérdést semmiképpen sem sza-
bad „kötelezően kitöltendő” mezőként kezelni, különösen azért
nem, mert ez az információ az úgynevezett különleges adatok kö-
zé tartozik.⁴ Nem haszontalan belegondolnunk abba, hogy mi tör-
ténne például akkor, ha a való életben kérdezné rá valaki a feleke-
zeti hovatartozásunkra. Olyannyira kényes kérdés ez, hogy még az
egyébként név nélkül zajló népszámlálás kérdőívére sem került rá.⁵

Még nagyobb lenne a (jogos) felháborodás, ha – tegyük fel – az
adóhatóság munkatársa kérdezné rá felekezeti hovatartozásunkra.
De a virtuális világban másként viselkedik a felhasználó. A való
életben „megedződött”, tudatos polgár gyakran különösebb kriti-
ka nélkül alkalmazkodik a virtuális világ körülményeihez: olyan
személyekkel oszt meg adatokat, akikkel esetleg nem szívesen ten-
né ugyanezt a való világban (vagy nem is gondol arra, hogy azok
hozzáférhetnek), és olyan adatokat tesz hozzáférhetővé, amelyek
megosztására egészséges öntudattal kellene nemet mondania – és
a való világban vélhetően határozottan nemet is mond. Szó sincs
üldözési mániáról, elég, ha végiggondoljuk, ki mindenki láthatja a
rólunk szóló információkat, néha igen változatos adatokat.

Másként fogadnak a munkahelyen vagy egy üzleti tárgyaláson valakit, ha a virtuális világban előzetesen tájékozódni lehetett róla. Mert ma már természetességgel tájékozódunk az interneten, és felkészülünk jövőendő kollégáinkból, tárgyalási partnereinkből. Visszatérve az előző példához: lehet pozitív vagy éppen negatív üzenete az adott közegben annak, ha valakiről a közösségi portálon megadott adatai alapján tudjuk: felekezeti középiskolába járt, vagy valamely párt képviselője mellett végzett szakmai gyakorlatot. Természetesen minden információnak lehet jóhíszemű és barátságos fogadtatása is, és a felhasználó talán ezzel találkozik a leggyakrabban (és ez lebeg a szeme előtt, amikor regisztrál), de a felhasználói közösség sokszínűsége és átláthatatlansága miatt óvatosságra kell inteni mindenkit. Meggyőződésem, hogy a közösségi oldalak közül is csupán azok lesznek hosszú távon is vonzó és versenyképesek, amelyek a felhasználók adatait a legszigorúbban védik, az adatok hozzáférhetőségét illetően a legvilágosabb szabályokat alakítják ki.

Nézzük az adatok megadásának másik oldalát: amikor az adataltany csupán önmagáról ad meg információkat, a jog nem szól közbe, mint jeleztük, felnőttként kezeli az adatok tulajdonosát. Itt jegyezzük meg: egyre több 18 év alatti is tagja a közösségi oldalaknak. Az érintett a rá vonatkozó adatok nyilvánosságra hozatalakor él információs önrendelkezési jogával (és nem visszaél azzal, mert saját adataira nézve ezt jogi értelemben nem is teheti meg). Kitöltetlenül hagyhatja az egyes mezőket, ha azonban mégis megválaszolja azokat, a jog nem kínál eszközt arra, hogy az adataltany döntését bárki megkérdőjelezze, csak ő gondolhatja meg magát utólag.

A virtuális arctalanság következményei

A virtuális világ számos olyan szolgáltatást is kínál, ahol a felhasználónak semmilyen módon sem kell magát azonosítania. Létrehozhat például egy e-mail címet anélkül, hogy valós adatokkal regisztrálna. Hozzászólhat egy fórumban a becenevén vagy álne-

ven. A közösségi oldalon profilt alkothat „összelopkodott” fényképekből, adatokból. A sort még hosszan folytathatnánk.

Azonosítás nélkül be tudunk tehát lépni a virtuális világba. Mások, akár jó-, akár rosszindulat vezérli őket, a többi felhasználó számára olyan adatokat tehetnek hozzáférhetővé rólunk, amelyek révén azonosítani lehet bennünket a való világban. A társke-reső oldalon más, valós személy nevében elhelyezett profil kényelmetlen helyzeteket eredményezhet, ha az érintett egyébként kiegyensúlyozott kapcsolatban él. Az internet egyes speciálisan védett felületeket (például az előzetes személyes regisztrációt igénylő ügyfélkapus belépést, banki tranzakciókat) leszámítva al-kalmatlan a felhasználó valódi kilétének megállapítására. Az in-ternet ugyanakkor lehetőséget ad arra, hogy mások számára is azonosítható személyekkel kapcsolatos információkat tegyenek közzé rajta. A felelősség utólagos megállapítása, éppen az arcta-lanság miatt, nagyon nehézkessé válik. Ez az ellentmondás első-sorban sajnos a rosszindulatú híresztelések, zaklatások terepévé változtathatja az adott felhasználó számára a virtuális világot, ahonnan azonban már nehezen tud kilépni a való világban őt sújtó érdeksérelmek nélkül (lásd Z. Karvalics László fejezetét). Sú-lyos sérelemnek nem csak a való életben bekövetkezett esemé-nyeket tekintjük, hanem annak kell tartanunk azt is, ha valakinek a virtuális közösségekben való részvételét nehezítik meg. A vir-tuális arctalanság tehát fokozza annak kockázatát, hogy az ebből fakadó szabadsággal visszaéljenek.

A XXI. század valutája: a személyes adat

Peter Schaarnak, a német szövetségi adatvédelmi hatóság veze-tőjének tulajdonítják azt a gondolatot, amely szerint a XXI. szá-zad egyik új valutája a személyes adat lesz. Az alkotmányos jogok védelmezőiként természetesen vissza kell utasítanunk minden olyan törekvést, amely az alapjogokkal összefüggésben értékesít-hető javakról beszél. Az említett idézetet nem is ilyen jelzésként,

hanem inkább figyelemfelhívásként kell értékelnünk, amely szerint az érintetteknek tudatosítaniuk kell azt, hogy személyes adataiknak értékük van, másoknak is megéri azokat „megvásárolni”, és erre akkor is gondoljanak, ha nem is érzékelik a személyes adatok szolgáltatásából adódó előnyöket vagy hátrányokat. Más megfogalmazásban: az egyén is becsülje meg személyes adatait, és csak akkor szolgáltatson adatokat magáról, ha látszik, hogy mit fog nyerni ezáltal, és az ajánlat számára „kedvező”.

A jog védelmének határai és az adatvédelmi jog kiegészítő szabályai

A virtuális világ valamennyire – mint érzékeltettük – a való élet megkettőződéseként működik. Az internetes közeg azonban gyakran olyan kommunikációs és tárolási lehetőségeket is nyújt, amelyek a való életben elképzelhetetlenek lennének. Az egyik ilyen rendkívül népszerű lehetőség a közösségi oldalakon való regisztráció, egy virtuális közösségben való részvétel. A fejezet elején leírtakat érdemes itt különösen is hangsúlyozni: egy ilyen közösségben (baráti közösségben) való részvétel – legalábbis első közelítésben – nem esik a jog érdeklődési körébe. Nem írja elő, hogy ki hogyan viselkedhet, egyáltalán: a jogszabályok a jogok és a kötelezettségek rendszerét nem határozzák meg egy ilyen közösségre nézve. A közösségi oldal üzemeltetője van abban a helyzetben, hogy bizonyos magatartási szabályokat megalkosszon, azokat a tagok számára elérhetővé tegye, és betartatásukra ügyeljen.

A személyes adatok kezelésének szabályozása a jog egészén belül a legszigorúbbak közé tartozik. Az adatvédelmi jog ugyanis nem megengedő módon szabályoz, mint más területeken szokás (mindent szabad, ami nem tilos), hanem éppen ellenkezőleg, csupán azt tekinti jogszerűnek, amire világos felhatalmazás van. Az adatkezelés területén ez azt jelenti, hogy a kötelező adatkezelést elrendelő törvény hiányában mindenki köteles az információs önrendelkezési jogot tiszteletben tartani. A közösségi oldalaknál mint példánál maradva az olyan fényképet például, ame-

lyen több személy látható, csak valamennyi érintett hozzájárulása birtokában töltheti fel a profiljára, és teheti mások számára hozzáférhetővé. Mihelyt tehát a felhasználó másik személy információs önrendelkezési jogának körébe tartozó döntést kíván hozni, a jog máris „bevonja” az esetet érdeklődési körébe, és a kötelező szabály követését várja el. A másokat is ábrázoló fényképek nyilvánosságra hozása a weben az egyik leggyakoribb adatvédelmi probléma.

A jogellenes adatkezelés „jó szándékkal” is megvalósulhat

A gondolatmenetet folytatva arra kell felhívni a figyelmet, hogy a személyes adatok védelmére vonatkozó szabályok megsértéséhez nincsen szükség feltétlenül a joggal vagy a jog által védett társadalmi értékekkel való tudatos szembehelyezkedésre. Sőt az „oszd meg másokkal is” hangulatában a felhasználó gyakran végig sem gondolja a nyilvánosságra hozás jogi vonatkozásait. A virtuális világ teremtette szabadságban sokan örömmel élnek a lehetőséggel, és mindenki számára hozzáférhetővé teszik például a nyaralásukról készült felvételeiket – olyanoknak is betekintést biztosítva ezáltal, akiknek egyébként talán nem szeretnék megmutatni, hiszen amikor a fotót hozzáférhetővé tesszük, a legritkább esetben gondoljuk végig, ki férhet majd könnyen hozzá.

Fontos tehát rögzíteni, hogy a személyes adatok engedély nélküli kezelése jelenti azt a határt, amelyet a jog irányadónak tekint, és az ezt átlépő magatartást már a jog is helyteleníti. Azért is kell ezt hangsúlyozni, mert például a fénykép (arckép) nyilvánosságra hozatalával nem feltétlenül valósul meg becsületsértés vagy éppen rágalmazás, önmagában sem szabálysértési, sem büntetőeljárást nem von maga után. Az egyén és adatai védelmére vonatkozó szabályok megsértése – ami ilyenkor megtörténik – azonban már elegendő súlyú ahhoz, hogy a jog a sérelmet szenvedettnek támogatást nyújtson. Nem nehéz belátni, hogy egy új párkapcsolatra nézve milyen problémákat okozhat, ha a közös-

ségi oldalon az előző partner profilján még látható a régi baráttal (barátnővel) készült közös fénykép, vagy éppen hogyan okozhat versenyhátrányt egy felvételi eljárás során az interneten „felejtett” bulizós kép. Ha az egyén érdekei sérülnek, akkor ez nem kerülheti el a jog figyelmét.

A becsület sérelmével járó cselekményeknél a személyes adatokat eszközként használják

Az érintettéről készült fénykép (vagy ahogy a jogszabályok említik, képmás) csak az érintett döntése alapján és annak megfelelően kezelhető. A web 2.0 világában az adatok forgalmának felgyorsulásával ez a jog szinte illuzórikusnak tűnhet, a személyiség védelme érdekében azonban épp emiatt is szükséges ennek hangsúlyozása. Az új környezetben nem csökken, hanem nő a jogi védelem jelentősége. A képmás védelme egyébként nem csupán a „Nyugat” hagyományaiban él: az iszlám és más vallások tradíciói is különös érzékenységgel tekintenek a személyiség e részének védelmére. Az esetek jelentős részében a felhasználót nem feltétlenül vezérelti rossz szándék, amikor a fényképet nyilvánosságra hozza. Hiszen lehet a kép szép emlék egy közös buliról, kirándulásról, ahol nem is gondolunk arra, hogy a háttérben még ki mindenki látható.

A jog másként értelmezi azokat az eseteket, amikor valaki kifejezetten mások becsületét, érdekeit sértő módon lép fel. Sajnos nem ritkák az olyan esetek, amikor az internetes közeget arra használják fel, hogy nagyszámú felhasználóhoz juttassanak el másokat lejárató üzeneteket (lásd Z. Karvalics László írását). Ezeknél a másra vonatkozó információk tipikusan eszközül szolgálhatnak a rágalmazáshoz vagy becsületsértéshez. A jog nyelvén: egy valós állítás, például intim helyzetben készült fénykép közzététele természetesen a személyes adatok védelmére vonatkozó szabályokba is ütközik, de elsősorban a büntetőjog körébe tartozik, és az információs önrendelkezési jog sérelme ilyenkor „beleolvad” a bűncselekménybe.

Az „információs önbíráskodásról”

Szintén gyakori jelenség, és az internet segíti ezt a lehetőséget, hogy a folyamatban lévő eljárások terheltjeit igyekeznek már az eljárás tényének nyilvánosságra hozásával kellemetlen helyzetbe hozni, esetleg, mivel nem bíznak a példás büntetés kiszabásában, mintegy „információs önbíráskodás” jelleggel járátva le másokat, önkényesen mennek elébe a jogi procedúrának. Mondanunk sem kell, hogy a jog tiltja az ilyen eljárást, és adott esetben az ilyen magatartás bűncselekménynek is minősülhet (általában a vádemelés az első olyan pontja a büntetőeljárásnak, amikor a terhelt neve jogszerűen nyilvánosságra kerülhet).⁶ Az ilyen jellegű híresztelések orvoslására rendelkezésre állhat a sajtó-helyreigazítás, ezt azonban a nem klasszikus sajtóorgánumok esetében nem lehet igénybe venni. A helyzetet bonyolítja, ha a közlésnek felületet adó szolgáltató minden felelősséget elhárít. Az egyén védelmét illetően a jog tehát itt is lépeshátrányban van: védtelenül hagyja azokat, akik a virtuális világban támadásnak vannak kitéve, és nincs hatékony (sem jogi, sem gyakorlati) eszközük az őket ért sérelmek orvoslására. Az „önbíráskodó” az arcatalanság mögé bújva el tudja érni célját, és a való életre is kiható kellemetlenséget tud okozni másoknak a becsületüket sértő kijelentések közzétételével.

A jog és a virtuális világ törvényszerűségei közötti különbségekre mutat rá az alábbi példa is. A bíróság nyilvános tárgyalásairól a sajtó jogszerűen adhat beszámolót, ismertetheti a vádlott nevét, a vádat, és jogszerűen kerülhet nyilvánosságra ezt követően a bíróság által hozott ítélet is. Ezek az információk természetesen az internetes médiumokban is közzétehetők, ahonnan utólag nagyon nehézkes egy-egy adat eltüntetése. Az információk elméletileg az „örök nyilvánosság” közegébe kerülnek, ahol egy névre rákeresve könnyedén elérhetők olyan elítélésre vonatkozó adatok is, amelyek már az erkölcsi bizonyítványban sem szerepelnek, mert a büntetőjogi mentesülés révén az elkövető már nem köteles elszámolni az adott büntetéssel. Az internet nyilván-

nossága tehát azzal a következménnyel járhat, hogy valaki büntetőjogilag mentesül ugyan, de ezt más szereplők felülírják, és a mentesülés eredeti funkciója (hogy az elítélt bizonyos idő eltelte után tiszta lappal indulhasson, és a társadalom hasznos tagjává váljon) nem érvényesülhet. A korábban elítélt személynek, ha valóban a tisztességes társadalmi boldogulás útját választja, és múltjától meg kíván szabadulni, nem marad más választása, mint a névváltoztatás.

A jogviszonyok keveredése, avagy vigyázat!

– munkáltatónk is jelen van a virtuális közösségben

Korábban már szoltunk az internet arctalanságának velejáróiról. Az arcnélküliség (tehát a való életben birtokolt jellemzők eltitkolása) csak egy bizonyos körig engedi az internet lehetőségeinek kihasználását. Egyes szolgáltatások, így jellegzetesen a közösségi oldalak, „arcunk” vállalása nélkül éppen a legfontosabb lehetőséget, a közösségi életet, ismerőseink megtalálását nem teszi lehetővé. Emiatt a felhasználók döntő többsége a való életben használt névvel regisztrál, így az arctalanság előnyei elenyésznek. A privátnak hitt szörfölés e ponttól kezdve társadalmi felelősséget követel. Nem gondolunk rá, de a munkahelyen, iskolában nem vállalt magatartást a virtuális közegben is kerülni kell (lásd Talyigás Anikó fejezetét).

Erre nem volt figyelemmel az a svájci munkavállaló, aki reggel telefonon azt jelezte munkáltatójának, hogy heveny szembebetegség miatt otthon kell maradnia, és az orvos utasításának megfelelően elsötétített szobában, minden fényforrást kikapcsolva kell pihennie. Ezt követően munkáltatója észlelte, hogy a „gyengélkedő” munkavállaló bejelentkezett az általa is használt közösségi portálra. A munkáltató félrevezetése a munkavállaló állásába került: nem számolt azzal, hogy munkáltatójával találkozhat a virtuális térben.

Az adatok minősége és a munkaerő-felvétel

Adatvédelmi törvényünk alapelvi szabályozást alkalmaz. Azokat az alapelveket fogalmazza meg a hazai jogi környezethez igazítva, amelyek a nemzetközi együttműködésekben az évtizedek során kikristályosodtak. Ilyen alapelv az adatok minősége. Ez azt jelenti, hogy a kezelt személyes adatoknak pontosnak, teljeseknek, és ha szükséges, időszerűeknek kell lenniük. Ezen túl szintén az adatok minőségének elvéhez tartozik az az elvárás, hogy az adatkezelés tisztességes és törvényes legyen.

Mindez az adatkezelőre ró kötelezettséget. Jogi értelemben különbség van a következő két eset között: a felhasználó önmagáról ad meg adatokat egy virtuális felületen, illetve az adatkezelő másokról kezel adatokat valamely jogviszony keretében. Az első esetben az érintettet nem terheli az a kötelezettség, hogy adatai minőségét garantálja, hiszen például a közösségi portálon elhelyezett profil tartalma jogi értelemben jogviszonyon kívüli adatkezelésnek számít. Az adatalany senkinek nem köteles számot adni az általa önmagáról elhelyezett adatok esetleges pontatlanságáról, valótlanosságáról. Nincs tehát jogkövetkezménye, ha a születési dátumát „elírja”, vagy például egy korábbi, előnyösebb küllemről árulkodó fényképet tesz fel magáról.

A második esetben az adatkezelő egy jogviszonyhoz szükséges adatokat kezel, nem önmagáról, hanem másokról, amely adatokra (ha természetes személyekre vonatkoznak) már alkalmazandó az adatvédelmi szabályozás minden előírása, így az adatminőség, a pontosság követelménye is.

Az internet világában egyidejűleg van jelen az arcnélküliség és a való életben hordozott azonosító jelek használata. Ahol szükség van az egyén való életben való azonosítására, ott az arctalanság az internet közegében sem alkalmazható. Ahol nincs szükség az azonosíthatóságra, mert a jogviszony ezt nem követeli meg, vagy éppen nem is beszélhetünk jogviszonyról, ott a virtuális világban (jogszerűen) lehet elrejtőzni az álszemélyiség mögé.

Egy ilyen közegben tehát nehéz bizonyosságot szerezni az adat helytálló voltáról, hiszen például egy közösségi oldalon adatlapot lehet létrehozni valakinek a nevében, vagy a neve alatt új e-mail címet generálni anélkül, hogy bárki a felhasználó személyazonosságát megállapítaná. Aki az interneten kíván az adott személyről tájékozódni, annak feltétlenül számolnia kell az adatok esetleges pontatlanságával.

Az egyénre vonatkozó információk sorsáról való tájékozódás az érintettnek az adatvédelmi törvényben biztosított joga. A web 2.0 világában, amikor a felhasználó már nemcsak letölt, hanem fel is tölt, az egyén nincs többé abban a helyzetben, hogy kövesse, ki, mikor, milyen adatokat hozott róla nyilvánosságra. A rossz szervezés és a kialakult szerencsétlen szokásrend eredménye lehet, hogy tudtunk és beleegyezésünk nélkül kerül nyilvánosságra egy konferencián elmondott előadásunk, egy nyilvánosságnak még nem szánt szakmai tervünk vázlata, egy készülőben lévő zenemű témája vagy egy félreérthető (félreérthetetlen?) helyzetben készült fényképfelvétel. Az említett esetekben, és még sok más esetben is úgy állhat elő a jogsérelem, hogy annak orvoslására kevés esély mutatkozik.

Óvatos becslés szerint is általános gyakorlattá vált a munkáltatók körében, hogy a felvételre jelentkező személyek interneten elhelyezett adatainak felhasználásával tájékozódnak az illető kvalitásairól és „egyéb” jellemzőiről. E kérdés vizsgálatának azért is van jelentősége, mert a munkaviszony jól szabályozott területe a jognak. A jogviszony szereplői, jogaik és kötelezettségeik pontosan meghatározottak, már a munkaerő-felvételre nézve is találunk szabályokat az igényelhető adatokra vonatkozóan.⁷

A munkáltató az interneten történő tájékozódás lehetősége révén valószínűleg olyan adatok birtokába jut, amelyek további megerősítést igényelnek, igényelnének. Jelenthet ez pozitív tapasztalatot: például szakmai anyagokat, de negatív dokumentumokat is az adott munkakörhöz nem illő nyilvános viselkedésről. Ha a munkáltató kizárólag a virtuális tudakozódás eredményeként megszerzett adatokra alapozza döntését, akkor az adatok

minőségét illetően nem tanúsítja az elvárható gondosságot, mert bizonyos tisztázást igénylő körülmények esetén nem adja meg az érintettnek a lehetőséget, hogy kifejtse álláspontját. A jövőendő munkáltató és munkavállaló között az olyan adatoknak, amelyek a jogviszonyt (vagy annak alakulását) érdemben befolyásolják, többek között az adatminőség elvének, a pontosságnak is meg kell felelniük.

A jelentkező kiszolgáltatottságát az is fokozza, hogy az életét később nagyban befolyásolni képes munkáltatójáról adott esetben csak az interneten tud tájékozódni. E fejtegetés jelentősége nem pusztán elméleti, hiszen, amint bemutattuk, az interneten elérhető adatok pontossága, hitelessége gyakran megkérdőjelezhető. Gondos körültekintéssel kell tehát vizsgálni a jogviszonyt befolyásoló adatokat. Az elvárható körültekintés elmulasztása esetén az adatkezelő eljárása nem felel meg a tisztességes adatkezelés kívánalmának. De a jogi sérelmen túl az egyén kiszolgáltatottsága, hiszékenysége alapján igen kellemetlen helyzetekbe sodródhat.

A közösségi portálokon elhelyezett információk böngészése során a munkáltatónak vagy a leendő munkavállalónak azt is figyelembe kell vennie, hogy a profil csupán az adott közösség számára nyilvános, nem bárki számára. Az adatok nyilvánossága tehát az adott közösségen belüli érintkezést szolgálja. Ha „halványan” tűnik is az adatok hozzáférhetőségét illetően e határvonal, a kellő körültekintéssel eljáró munkáltatónak észre kell vennie, és nem szabad azt átlépnie. Amint azt az egyik fenti példában említettük, a munkáltató (vagy személyzetis) is lehet felhasználó, és semmiképpen sem tekinthető jogi értelemben helyteleníthetőnek, ha éppen egy közösségi portálon „találkozik” a munkavállalójával. A munkaerő-felvételnek azonban jogilag szabályozott mederben kell maradnia, és ha a jelentkezőt az általa nem a munkavállalás céljára megadott adataiból levont következtetések révén éri hátrány, akkor a munkáltató valójában megkerüli azt az utat, amit a jog kijelölt. Ennek egyik veszélye, hogy a munkáltató téves következtetést von le az egyébként sem megbízható forrású infor-

mációkból, másrészt pedig a munkavállalót fosztja meg a jog által biztosított védelemtől azáltal, hogy a jogszerűen igényelhető adatokon túl is betekint magánszférájába.

Említettük, hogy a felhasználó profiljába való betekintés tilalma a jogban „halvány” határvonallal kijelölt magatartás, ugyanakkor a magánszféra körébe tartozó adatokkal való bánás fokmérője lehet az adott szervezeti kultúrának. Az is kétségtelen, hogy a munkavállaló egy ilyen helyzetben nagyon nehezen tudja orvosolni az őt ért (vagy vélhetően ért) sérelmeket. Talán akkor a legjobban definiált a jogorvoslat lehetősége, ha a munkavállaló szerint az egyenlő bánásmód követelménye sérült, ilyen esetben ugyanis az eljárás során a munkáltatónak kell igazolnia, hogy jogszerűen járt el. Tudnunk kell: ha az önkorlátozás nem érvényesül ezen a téren, akkor a jog nehezen ad iránymutatást a munkavállaló, vagy adott esetben a munkáltató érdekeit sértő döntések kapcsán.

Ez a példa is az internet mint megbízható forrás egyre inkább terjedő gyakorlatára világít rá, jelezve, hogy a felhasználó akkor jár el helyesen, ha az önmagáról elhelyezett információkat vagy az azokhoz hozzáféréssel rendelkezők körét erőteljesen korlátozza a virtuális térben. Megjegyezzük: a munkáltatónak a jogi korlátozáson túl belső erkölcsi megfontolás alapján is döntenie kell, mikor, hol, milyen, a birtokába jutott ismeretet használ fel, amikor emberek sorsáról dönt, vagy legalábbis befolyásolja azt.

Az interneten hagyott nyomaink felhasználása

Eddig arról értekeztünk, hogy a felhasználó által a virtuális közegben magára vagy másra vonatkozó adatok kezelésének milyen jogi következményei vannak. A felhasználó az interneten rengeteg olyan információt hagy maga után, amelyek sokat érnek a szolgáltatók, piaci szereplők számára. Az internetes nyomok kapcsán lényeges, hogy különbséget tegyünk az egyénekhez nem kapcsolható, és az egyes felhasználókkal egyértelműen kapcsolatba hozható információk, adatok között.

Az első esetben (amikor az információk nem köthetők egy adott felhasználóhoz) gyakorlatilag statisztikai jellegű adatgyűjtésről beszélhetünk, ahol nem a felhasználók kiléte, hanem azok „dabszáma”, vagy jellemzőik előfordulása fontos. Ha az adatokat nem kívánják az egyes felhasználókhoz kapcsolni, akkor az adatok kezelése nem esik adatvédelmi szabályozás alá. Ha azonban az adatok konkrét személyekhez kötése megtörténik, akkor jogi értelemben véve fontos határvonalat lépnek át az adatkezelők, hiszen az anonim adatok helyett már személyes adatokra kíváncsiak, amelyek az adatkezelés teljes ideje alatt a jog védelme alatt állnak.⁸

Az online világban a felhasználó magasabb szintű, azaz személyre szabott kiszolgálása legitim célkitűzés. Ehhez azonban személyes adatok felhasználása is szükséges lehet. Ez jogszerűen csak az érintett személy hozzájárulásával oldható meg. E körben az egyik legnehezebben megoldható problémát az okozza, hogy nem tisztázott, milyen módon adhatná az érintett hozzájárulását adatainak személyre szabott üzenetek eljuttatásához szükséges kezeléséhez. A hozzájárulás történhet-e egyfajta „csomagban”, és a tájékoztatásnak mire kell kitérnie, milyen módon kell ezt a felhasználó rendelkezésére bocsátani? E kérdésekre könyvünk írásának idején is keresi a választ például az Európai Unió 29-es Adatvédelmi Munkacsoportja.

Adatbányászat⁹ – a törvényesség határán innen vagy túl?

A fejezet kereteit nyilvánvalóan meghaladná e téma részletesebb kifejtése. Ha az adatbányászatnak a magánszférát érintő vonatkozásait röviden össze kívánjuk foglalni, akkor úgy fogalmazhatunk, hogy ez a tevékenység az adott közösségről (fogyasztókról, ügyfelekről stb.) kezelt adatokban rejlő, nem nyilvánvaló, addig nem ismert következtetések levonására irányuló eljárás. Az eljárás során személyes adatok kezelése történik, amennyiben az eljárás célja személyre lebontott következtetések levonása, vagy az eljárás ehhez vezethet. Példa erre a fogyasztási szokások vizsgálá-

lata, amikor az elemzés alapján lehet jobb szolgáltatásokat kialakítani. Egyesek szerint az adatbányászat természeténél fogva folyamatosan próbára teszi a jog tűrőképességét. E tevékenység nem tekinthető a törvényesség határán túlra (jogellenesnek), amennyiben folyamata az érintettek számára ismert, és felette valamilyen kontrollt tudnak gyakorolni (hozzájárulhatnak vagy tiltakozhatnak ellene). Hangsúlyozandó, hogy mind a strukturált, mind a strukturálatlan adatokban rejlő következtetések legitim célok szolgálatába állíthatók, és helyes, ha ezzel a lehetőséggel élnek a magáncégek, de akár a közigazgatás szervei is. Az adatok „bányászata” tehát mindaddig a törvényesség határán belül marad, amíg az adatalanyok tudnak az őket is érintő tevékenységről és annak lehetséges következményeiről. Az esetek többségében azonban ez nem ismert, így tiltakozni is nehéz ellene. A regisztrációk során csak úgy észrevétlenül, a kérdésekre – például: Mi a hobbink? Hol lakunk? Hány évesek vagyunk? – válaszolva segítjük elő e tevékenységeket. De mint szó volt róla, ezen elemzések eredménye az esetek többségében a felhasználónak nyújt jobb kiszolgálást, s így természetesen a szolgáltatónak nagyobb bevételt.

Az adatmegőrzési irányelvből folyó kötelezettségek: konfliktus a célhoz kötöttség elvével

A virtuális térben kifejtett magatartásunkról árulkodó nyomok nem csak az üzleti világ, hanem a bűnüldöző hatóságok munkáját is elősegíthetik. Az adatmegőrzési irányelv¹⁰ megalkotása az európai adatvédelmi jog szempontjából azért jelentett különleges kihívást, mert gyakorlatilag nyíltan szembehelezkedik a célhoz kötöttségről eddig alkotott általános vélekedéssel és gyakorlattal. Az irányelv arra kötelezte az uniós tagállamokat, hogy az elektronikus hírközlési szolgáltatók számára a forgalmi adatok meghatározott ideig történő megőrzését írják elő bűnüldözési célból (6–24 hónap, ezen belül a nemzeti jogalkotó szabadon dönthetett). Az elektronikus hírközlési szolgáltatónak az irányelvnek megfele-

lő szabályok alapján már nem csak akkor kell eleget tennie az adatigénynek, amikor az adat a hatóság kérése esetén rendelkezésre áll (mert a szolgáltatáshoz kapcsolódóan az egyébként megtalálható a szolgáltató adatbázisában), hanem már előre fel kell készülnie arra az esetre, ha a hatóság adatigénnyel lépne fel, és bizonyos típusú adatokat kérne. A célhoz kötöttség fényében különös, hogy a jogalkotó olyan feladat (a bűnüldözés) kiszolgáltatására kötelezi a szolgáltatót, amely idegen annak eredeti feladataitól.

A különböző szervezetek funkcióinak összeecsúszásával jár a szabályozás, amely adatvédelmi jogi elemzésünk alapján valóban nehezen békíthető össze a célhoz kötöttség elvével. Ez az uniós irányelv azt a kötelezettséget rója az elektronikus hírközlési szolgáltatóra, hogy egy másik szereplő kötelezettségeinek teljesítése (a bűnüldöző hatóság tevékenysége) érdekében tároljon adatokat meghatározott ideig.

Az adatvédelmi jog művelői nagy érdeklődéssel várták az első, e tárgyban született nemzeti alkotmánybíróági határozatokat. Ezek között volt olyan, amelyik megsemmisítette az irányelv nemzeti átültetését szolgáló jogszabályt (például Romániában), ugyanakkor a még nagyobb érdeklődéssel várt német szövetségi határozat sokakban csalódást keltett. Igaz ugyan, hogy a testület megsemmisítette az adatmegőrzést előíró jogszabályt, de azt is kinyilvánította, hogy az adatmegőrzés kötelezettsége alkotmányos keretek között megvalósítható, tehát annak gondolata összeegyeztethető a német alaptörvénnyel.¹¹ Úgy tűnik, teljesül az európai jogalkotó akarata, és a bűnüldözés érdekében az adatmegőrzés kötelezettsége Európa-szerte elfogadottá válik.

A bizalom hiánya a virtuális közegben – a felhasználó tájékozódása és tájékoztatása

Ha az eddigieket összegezve, az egyén helyzetét vizsgálva a jogkereső polgár igényeit kívánjuk megfogalmazni, azt látjuk, hogy alapvetően két fontos követelményt támaszthat: magyarázzák el

neki egyrészt azt, hogy mi zajlik a (virtuális) világban, másrészt azt, hogy milyen jogaik és kötelezettségeik vannak ott az egyes szereplőknek.

Az első követelmény egy jól szervezett társadalomban az oktatás és a tömegtájékoztatás segítségével nagyrészt megvalósul. A második követelmény teljesülése sokkal nehezebb. Ez függ azoktól a szervezetektől, magán- és jogi személyektől, akikkel a polgár különböző kapcsolatokba kerül a virtuális világban. A végigolvaszhatatlanul hosszú szerződések a virtuális világban folyamatosan kattintgató felhasználó számára szinte fel sem tűnnek, és elfogadásukra – általában olvasás nélkül – már rá is kattint. Hasonló könnyedséggel fogadja el az elolvasatlan adatvédelmi szabályzatot is, s mindezek ismerete nélkül lép üzleti kapcsolatba adattait megadva az új szolgáltatóval. Természetesen nem túlzó elvárás, hogy a szolgáltató közérthető, rövid, mégis minden lényeges feltételről beszámoló anyagokat tegyen fel weblapjára. A játékszabályok ismerete, ismertetése nélkül – jogilag – nem várható el az érintett együttműködése.

A való világ viszonyaira nézve igaz, a virtuálisra pedig különösen is igaz az a megállapítás, hogy mind a tájékozódás, mind a jogviszonyok gondos megválogatása, azok befolyásolása aktív magatartást követel(ne) a felhasználótól is. Az információs önrendelkezési jog jellegénél fogva „magára hagyja” a polgárt, a jogi környezetnek megfelelően neki kell a döntéseket meghoznia személyes adatairól. Az adatalany tehát maga dönt saját adatairól, majd a szolgáltatások igénybevételéről, s ez a felelősség alapos körülményt indokol.

A fentiekben azokat a kérdéseket taglaltuk, amelyek személyes adataink védelmét a virtuális közeg sajátosságaira tekintettel érintetik. Sajnálatos, hogy a virtuális világ a személyes adatok kezelését illetően egyelőre kockázatos környezetként él sokak szemében. Az adatainkra, és ezáltal érdekeinkre leselkedő veszélyeket komolyan kell venni. Egyes becslések szerint az internetes bűnözés „összjövedelme” meghaladja a kábítószer-kereskedelem volumenét. Ennek ismeretében az Európai Unió illetékesei azt fontolgat-

ják, hogy egy központi koordinációs szervet hoznak létre a tagállamok kiberbűnözés elleni küzdelmének összehangolására.

Szintén a bizalomvesztésre adott uniós válasz az úgynevezett Digital Agenda. Az Európai Unió Bizottságának illetékes főigazgatóságai által létrehozott honlap¹² a felhasználók tájékozódásának lehetőségét hivatott elősegíteni a Digital Agenda jegyében. A program célul tűzi ki a kéretlen e-mailek (spamek) elleni határozott küzdelmet, a digitális tartalmak egységes védelmét (szerzői jogi eszközökkel), egyben jogbiztonságot kíván nyújtani a felhasználónak abban, hogy az adott tartalommal mit tehet és mit nem (mit másolhat, tölthet le). A Digital Agenda kiterjed a magánszféra védelmére, a tisztességes szerződéses kikötésekre, a fogyasztókkal élők joggyakorlásának elősegítésére, az online fizetések iránti bizalom erősítésére, és a kereskedelmi védjegyek világhálón való elterjesztésére. A Digital Agenda tehát nem tűz ki más célt, mint azt, hogy a világháló a közjót, mindenki javát szolgálja. Személyes adataink védelme szempontjából nem a virtuális világtól való távolmaradás, hanem annak biztonságos használata jelenti az előremutató megoldást, ahhoz azonban, hogy ez megvalósuljon, valamennyi szereplő együttműködésére szükség van.

Az érintetlen magánszféra gondolata egyre távolabb sodródik a napi valóságtól, és ahogyan a tiszta környezettel kapcsolatban már bele kellett törödnünk, hogy csak a közszféra és a civil összefogás tevékeny együttműködése hozhat eredményt, úgy magánszféra védelme kapcsán is meg kell barátkoznunk a gondolattal: a virtuális magánszféra magától nem, csak a mi tevékeny részvételünkkel, körütekintő magatartásunk révén valósulhat meg.

Rácz Bencze *A Fusiongate Kft. ügyvezetőjeként és vezető tanácsadójaként dolgozik, főként biztonsági auditokat, tanácsadást és etikus hackelési projekteket vezet*

WE WATCH YOU WATCH¹

Tegyük fel, hogy Péter üzleti levelezése a Gerda nevű ingyenes postafiók-szolgáltatónál található. Ennek jelszavát rendszeresen változtatja, a jelszó most: Solyom17.

Péter emellett a Fancom nevű ingyenes postafiók-szolgáltatónál bonyolítja alacsonyabb prioritású levelezését, ide irányítja a különböző közösségi oldalakról és hírlevelekről érkező leveleket, amelyekre éppen csak néha néz rá. Példánkban közismert tény ugyan, hogy a Fancom rendszere nem a legbiztonságosabb a világon, de az itteni jelszava Szalonka28, így semmi esély nincs rá, hogy a Gerdánál lebonyolított fontos üzleti levelezéséhez bárki is hozzáférjen, még ha feltörik is a rendszert, más a jelszó.

A nem túl jó hírű Fancomnál ismét biztonsági incidens történik, amelynek során a hacker technikás, és nem az a fajta, aki nagydobra verné a sikerét, így, ahogyan a valódi hackerek teszik, láthatatlan marad.

Péter üzleti levelezéséhez más volt a jelszó, ezért Péter biztonságban van, hiába törték fel a Fancomot.

Ez az írás az ilyen és hasonló jellegű problémákról szól – amellet, hogy elmondjuk, milyen veszélyek leselkednek példánkban Péter cégének adataira, megmutatjuk az olvasónak a jelszavak általános gyengeségeit, és elmondjuk, hogyan lehet megoldani a biztonságos azonosítást a számítógépes rendszereken. Ezenkívül tisztázzuk a *hacker* szó definícióját és a szó által takart különböző szubkultúrák morális hátterét, egymáshoz való viszonyát, áttekintjük a hacker személyiségprofilját és társadalmi beágyazódását. Végül, mielőtt megtanulnánk „a hacker fejével gondolkodni”, áttekintünk néhány olyan módszert, amelyet hackerrek alkalmaznak arra, hogy konkrét célpontokat támadjanak meg, és így akár országok közti viszályok idején a háborús diplomácia eszközeivé váljanak.

A jelszavak legsúlyosabb veszélye – amiről mindenki hallgat

Nézzük meg, hol rejlik potenciális biztonsági incidens a fejezet elején megadott példánkban.

A Fancomot működtetők csak fél év múlva veszik észre a biztonsági incidenst. E fél év során a hacker a weblap azon részét, amely a belépéseket bonyolítja, egy olyan kis szoftverrel látja el, amely eltárolja az összes jelszópróbálkozást, amely a Fancom belépési rendszerében történt, majd természetesen továbbítja azokat a Fancom rendszerének. Így ha a jelszó helyes volt, akkor a beléptetés teljesen üzemszerűen meg is történik.

Egy fontos momentumra hívom fel a figyelmet: eltárolja az összes próbálkozást. A hibás próbálkozásokat is.

A problémák akkor kezdődnek, amikor Péternek egy leterheltebb időszaka következik a munkában, ezért elsősorban az üzleti levelezését használja leginkább, így kevés ideje marad rá nézni a hírlevelekre és közösségi oldalakra. Azonban a terhelés egyszer csökken, és Péternek kedve támad olvasgatni a másik

e-mail címén is. Amikor belép, akkor Fancom loginkérő oldalán a felhasználói nevet helyesen tölti ki, azonban a jelszókérésnél rutinosan beírja a Solyom17-et. A Fancom visszadobja a hibás jelszót, és Péter második vagy harmadik próbálkozásra „mi is volt ide a jelszavam?” felkiáltással végigpróbálja az összes jelszót, ami eszébe jut, és egy idő után sikeresen belép a Fancom rendszerébe.

A hackernek pedig, ha Péter cégének adataira fáj a foga, már csak azt kell kiderítenie, hogy Péter cégének levelezése melyik szolgáltatónál van, hiszen Péter összes jelszavának birtokában van, annak ellenére, hogy csak az egyik olyan rendszert törte fel, amelyhez Péternek hozzáférése volt.

A jelszavakkal kapcsolatos legsúlyosabb veszély tehát: egy megjegyezhető, változatlan karaktersorozatra bízunk az azonosítást. Hiába változik a karaktersorozat a különböző rendszerek közt, és hiába változtatja a felhasználó a legfontosabb üzleti levelezését védő jelszót rendszeresen, ha az egyik rendszert, amelyhez a felhasználónak köze van, feltörik, akkor az azonosítás biztonság az összes rendszeren kompromittálódhat.

A hackerek pedig, ezt tudva és okosan kihasználva, gyakran tartanak fenn olyan adatbázisokat, amelyek rengeteg ember adatait tartalmazzák: e-mail cím; a rendszer neve, amelyet feltörték; felhasználónév; jelszó és az összes többi „elgévelt” jelszó. Így szépen lassan egy-egy igen nagy hatalommal – összegyűjtött adatbázissal – rendelkező hacker kezében összpontosul az összes rendszer összes felhasználójának összes adata. Ezek felhasználásával, ha valamilyen oka van rá, bármikor továbbléphet, és olyan rendszerekhez is könnyedén hozzáférhet, amelyek még nincsenek az uralma alatt.

Ez a jelszavak legsúlyosabb veszélye, amelyről senki sem beszél.

A jelszavas azonosítás alapvető gyengesége tehát még egyszer: egy változatlan karaktersorozatra bízunk az azonosítást, a felhasználó azonosítását. Láthattuk, hogy ez a karaktersorozat változhat a különböző rendszerek közt, sőt a gondos felhasználó

a legfontosabb üzleti levelezését védő jelszót rendszeresen változtatja is. Így biztonságban érzi magát. A biztonság ilyen illúziója azonban hamis.

A jelszó

A jelszó, az informatikával és az információbiztonsággal csak felületesen érintkezők körében, általában a biztonság szinonimája. Ha egy fájl, egy rendszer vagy egy eszköz „jelszóval van védve”, akkor az onnantól kezdve bizonyára feltörhetetlen, hozzáférhetetlen, megbízható lesz, gondolják sokan! Így van? Nézzük meg a kérdést közelebbről.

A jelszó esetében egy olyan karaktersorozatra bízunk az informatikai rendszerek védelmét, amelyet egy ember képes fejben tartani. Hogyha egy ember képes megjegyezni, akkor képes továbbadni, leírni, vagy ha kényszerítjük, akkor leírja akkor is, ha tudatosan nem jutna eszébe ilyet tenni.

De ha nem történik semmiféle külső beavatkozás, a jelszó akkor is egy hihetetlenül gyenge módszer, amely mellett alkalmaznunk kell sok egyebet is, ha valóban meg szeretnénk védeni adatainkat. Mégis, nap mint nap rengetegen bíznak jelszavakra olyan adatokat, amelyek rossz kezekbe kerülve hatalmas károkat okozhatnak gazdasági társaságoknak, szervezeteknek és magánszemélyeknek egyaránt.

Magyarországon a legnagyobb jelszó-mintavételezésre lehetőséget adó biztonsági incidens az előző évezred végén történt. Ennek során több mint 33 000 magyar átlagfelhasználó jelszavának titkosított változata került a biztonsági szakemberek és a hackerok kezébe. Ebből kitűnően látszik, hogy a legtöbbször használt jelszavak magyar keresztnév (tamas, andras), becenevek (laci, apuci), főnevek (almafa, szerda, buda, joe, cat), tehát tipikus angol és magyar szótári szavak, vagy a loginnév módosított verziói (szabog esetén gszabo vagy gszabog). Gyakran fordulnak elő a felhasználónév tulajdonosának nevével kapcsolatos variációk (pl.

zsuzsanna / kiss), a loginnévvel kapcsolatos variációk, vagy éppen a variáció hiánya (gszabo / gszabo).

Hogyan kerüljük el a rossz jelszót

Jelszavunknak ne legyen köze a felhasználó valódi nevéhez, ne legyen köze semmilyen tulajdonnévhez, állat nevéhez, ismétlődő karaktersorozathoz, baráthoz, rokonhoz. Jelszavunknak ne legyen köze a QWERTY billentyűzet bármilyen egymás mellett található karaktereinek sorozatához, autórendszámhoz, irodai, otthoni vagy mobiltelefonszámhoz, hírességhez, káromkodáshoz, bármilyen nyelven használt szóhoz, ígéhez, főnévhez, születési dátumhoz vagy bármilyen valós vagy valótlan személy személyes adatahoz, vagy ezek bármilyen eltorzított verziójához (beleírva számot, vagy fordítva írva). Rossz jelszavak például az egyszerű számokkal kiegészített jelszavak (anyu1), az egyszerű számokkal behelyettesített betűket tartalmazó jelszavak (b0r1ska), az ismétlődő szavak (macimaci) is.

Ezekén kívül még nagyon sok szempontból lehet egy jelszó gyenge.

A jó jelszó

A jelszó legyen legalább nyolc, de ha a rendszer lehetővé teszi, akkor lehetőleg tizenkét-tizennégy karakter, tartalmazzon számot, kisbetűt, nagybetűt, speciális karaktert (!@#\$\$%^&*). A jelszóban legyen egy darab egymás után ismétlődő karakter. Ne legyen több, azaz ne háromszor ismétlődjön. Így, ha megfelelő sebességgel gépelünk, a vállunk mögött leskelődő támadó (*shoulder surfing*) sem lesz képes belépni a rendszerbe a nevünkben.

Jó jelszó lehet például: hR#2!iie\$*_?f – van benne kisbetű, nagybetű, szám és speciális karakterek. Ez azt feltételezi, hogy a támadónak egy nagyobb méretű karaktertáblával kell dolgoznia ahhoz, hogy feltörje a jelszavunkat. Komoly probléma, hogy ezt a

jelszót nehéz, sőt szinte lehetetlen megjegyezni, ezért a felhasználó jó eséllyel le fogja írni. Belátható azonban, hogy négy-öt ilyen karaktersorozat memorizálásával és kismértékű variációjával sok évig aránylag biztonságos jelszóval lehet védeni adatainkat. Lehet alkalmazni különféle módszereket is ezek megjegyzésére – minden karaktert össze lehet kötni valamilyen módon logikusan, és ezáltal bármilyen karaktersorozat megjegyezhetővé válik.

Az eddigiek alapján talán már a témában kevésbé járatos olvasó számára is levonható a következtetés, hogy a jelszó nem a legalkalmasabb módszer az adatok védelmére vagy személyek digitális módon történő azonosítására. Jelenleg azonban ez a legelterjedtebb módszer, ezért rá vagyunk kényszerítve használatára. Ha így van, akkor legalább válasszunk biztonságos jelszót, ugyanis is egy támadás esetén ezen nagyon sok múlhat!

Mégis, mennyi idő?

Brute force-nak, azaz „nyers erő”-t alkalmazó támadási módszernek nevezzük azt, amikor a támadó a jelszó összes karakterét egyesével végigpróbálgatja, A-tól Z-ig és 0-tól 9-ig stb.

Azért rendkívül fontos, hogy hét-nyolc karakterből álljon a jelszó, és hogy többféle karaktertáblát használjon, ne csak kis-

Karaktertábla	Szimbólumok száma a karaktertáblában	3 karakteres jelszó		6 karakteres jelszó	
		Próbálkozások száma	Időmennyiség	Próbálkozások száma	Időmennyiség
a-z	26	17 576	0,02 mp	308 915 776	5 perc
a-z és 0-9	36	46 656	0,04 mp	2 176 782 336	36 perc
a-z, A-Z és 0-9	62	238 328	0,2 mp	56 800 235 584	15 óra
a-z, A-Z, 0-9 és pontuációs karakterek	94	830 584	1 mp	689 869 781 056	8 nap

1. táblázat. A jelszótörés sebessége – másodpercenként 1 000 000 próbálkozással számolva *brute force* módszerrel, az összes lehetőséget sorrendben végigpróbálva

8 karakteres jelszó		12 karakteres jelszó	
Próbálkozások száma	Időmennyiség	Próbálkozások száma	Időmennyiség
208 827 064 576	58 óra	95 428 956 661 682 176	3000 év
2 821 109 907 456	32 nap	4 738 481 338 321 616 896	150 000 év
2 183 40 105 584 896	7 év	3 226 266 762 397 899 821 056	100 millió év
6 095 689 385 410 816	193 év	475 920 314 814 253 376 475 136	Több, mint amennyi ideje bolygónk létezik

Az 1. táblázat folytatása

betűket és számokat tartalmazzon, mert egy hozzáadott karakterrel a feltörésre szánt számítási kapacitás és a szükséges időmennyiség nem lineárisan, hanem exponenciálisan nő.

Így, mint az 1. táblázat alapján is megállapítható, a „szandi1” és a „sZ4nD!1.” jelszavak közt *brute force* módszer alkalmazása esetén pontosan 193 év különbség van, amennyiben 1 000 000 jelszóval próbálkozunk minden másodpercben, az összes lehetőséget sorrendben végigpróbálva. Kiemelendő, hogy az utóbbi, személynévhez hasonlító jelszó lévén, még mindig nem javasolt biztonságos jelszoválasztásnak.

A jelszóprobléma megoldása: a többfaktoros azonosítás

A jelszóval kapcsolatos alapvető problémák, ahogyan az informatikában a legtöbb tényezőnél, itt is az infrastruktúrában rejlenek: azaz magában a módszerben rejlik a hiba.

Némiképp biztonságosabbnak mondhatjuk azokat az azonosítási módszereket, amelyek több tényezőt vesznek figyelembe az azonosítás kivitelezésekor. Ilyen faktorok lehetnek a tudás alapú, birtoklás alapú és biometrikus alapú hitelesítési módszerek. Ennek példája, amikor egy internetes banki szolgáltatás igénybevételekor a loginnév és jelszó páros helyes megadása után (tudás a partner

mobiltelefonjának száma) a felhasználó a mobiltelefonjára kapott hitelesítő jelszóval (birtoklás) két különböző információs csatornán történő hitelesítéssel bizonyítja a rendszerekhez való hozzáférési jogosultságát.

Mi az a „kulcs”?

Létezik egy jól kidolgozott, de kevésbé elterjedt azonosítási rendszer, a kulcsos vagy elektronikus aláírás.² A kulcsos azonosítás nagyon leegyszerűsítve azt jelenti, hogy az azonosításhoz több véletlenszerű karaktersorozatot használunk, amelynek hosszúsága a 2 valamelyik hatványa – általában 128 és 2048 karakter között.

Az érdekesség kedvéért néhány statisztikai adat: Ahhoz, hogy egy darab 128-bit hosszú szimmetrikus kulcspár³ minden lehetséges értékének felvételére kísérletet tegyünk (*brute force* támadás), 2^{128} lehetőséget kell végig próbálnunk. Ez egészen pontosan 340 282 366 920 938 463 463 374 607 431 768 211 456 lehetőséget jelent. Egy olyan eszköz, amelyik képes lenne egy milliárd milliárd (10^{18}) lehetőség ellenőrzésére másodpercenként, pontosan 10^{13} év alatt számolna ki ennyi lehetőséget. Ez az univerzum becsült korának (13 milliárd év) az ezerszerese.

E feladat a fizika jelenlegi állása szerint az úgynevezett Von Neumann–Landauer-határ miatt a számítási kapacitás és a felvett energiaigény alapján, az informatika jelenlegi eszközeivel gyakorlatilag lehetetlen.

Nem is olyan bonyolult

A komolyabb üzleti rendszerek között már elterjedtek azok a kulcspárokat használó azonosítási módok is, amelyek szintén tudás és birtoklás alapú azonosítást használva, a jelszó mellett privát és publikus kulcspárokkal azonosítják a felhasználót. A mód-

szer többek között azért nem terjedt el minden rendszerre, mert a működtetéséhez szükséges informatikai infrastruktúra sokkal komplexebb, drágább, mint a hagyományos jelszavas azonosítás esetén. A kulcsos azonosítás esetén a kommunikáció a partnerek között még akkor is bonyolultabb, ha a felhasználók kezébe kulcsot tartalmazó tokent adunk a privát kulcs tárolásához.

A megoldásnak azonban nem szükséges bonyolultnak lennie sem a kommunikáció, sem az informatikai infrastruktúra szempontjából. Elég, ha az érzékeny adatokkal rendelkező cég olyan központi hitelesítő szervert hoz létre, amely egyszerre két faktor alapján valósítja meg az azonosítást (ez lehet: kulcspár, token vagy mobiltelefon sms-küldés útján), és az azonosított számára így az összekapcsolódást lehetővé tenné az alrendszerekkel, amelyek eddig „csak jelszót” kértek. Itt jegyzem meg, nincs olyan cég, magánember, amely/aki ne rendelkezne érzékeny adattal (lásd Szabó Endre fejezetét), s féltő, hogy ez számítógépes rendszereikre is igaz.

Ezzel a módszerrel hosszú távon kiküszöbölhető a teljes jelszólopás és az adott felhasználók lopott jelszavaival további rendszerek feltörésének jelentős része, hiszen arra már kisebb az esély, hogy a rendszer feltörése után a hacker a felhasználó mobiltelefonját is meg tudja szerezni.

Ki a hacker?

A *hacker* szó jelentése a szót használó különböző médiumok esetén a médium szakmaiságától függően gyakran jelentős eltérést mutat. Ez a különbség sokszor heves vitákat szül az informatikai szakma képviselői és az informatikához csak érintőlegesen vagy egyáltalán nem kapcsolódó körök közt. A szó értelmének többféle szakadása annak köszönhető, hogy a média számára csak egy bizonyos fajta hacker tevékenysége hírértékű és észlelhető, ennek megfelelően pedig a média a szót – az informatikai szakmai közösségek számára derogáló módon – ezzel a típussal azonosította.

Ez a típus az, aki önös érdekből mások informatikai rendszereit feltöri. A valóság azonban – nemcsak az önös érdek változatossága, hanem a rendszerek szempontjából is – ennél sokkal színesebb.

Tekintsük át, ki mit ért a hacker fogalmán!

A szakmai közösségek terminológiája

Hackernek nevezzük azokat a rendkívüli technikai tudású informatikai szakembereket, többnyire szoftverfejlesztőket, a nyílt forráskódú rendszerek elhivatott támogatóit, akik az informatikai rendszerek működését az általános rendszergazdai és szoftverfejlesztői szint felett ismerik, és az informatika bizonyos ágait rendkívül magas szinten művelik. Gyakran ők hozzák létre az azokat az eljárásokat (pl. RFC-k),⁴ amelyek definiálják az internet és az informatika alapjait. Olyan szakemberek, akik az informatikai biztonsági rendszerek megkerülésére specializálták tudásukat. A hackereken belül megkülönböztethető:

1. *Blackhat*: számítógépek illegális feltörésére, információlopásra, üzleti hírszerzésre specializálódik;
2. *Whitehat*: a biztonságtechnika fejlődésére és a hibák javítására helyezi a hangsúlyt;
3. *Greyhat*: erkölcsileg egyik irányban sem elkötelezett;
4. *Cracker*: szoftverek illegális módon történő technikai használhatóvá tételével, „feltörésével” foglalkozik.

A *blackhatek* számára derogáló a biztonságtechnikával foglalkozó közösséggel való párhuzam, ezért ez a csoport ezt „kikéri magának”. A szavak értelmezését tovább bonyolítja, hogy ez a csoport szakmai tudástól és erkölcsi beállítottságtól függetlenül cinikus módon általánosítva a *cracker* szót használja a fent *whitehat*ként definiált hackerekre és a *script kidekre* egyaránt. A médiában és a különböző közösségek szóhasználatára a két különböző szubkultúra összemosása jellemző.

Script kid: Rosszindulatú, csekély technikai tudású kezdő hacker vagy informatikai szakember. Jellemzője, hogy a céljai ha-

szonszerzés, szórakozás vagy akár oktan károkozás. A feltört weboldalakról, rendszerekből információt lop. Tudását többnyire a *whitehat* hackerek publikációiból meríti, így nem is érti igazán, mit is csinál pontosan.

A média terminológiája

Ennek megfelelően tehát amikor egy általános médium a hacker szót használja, akkor többnyire azt az utóbbi (*script kid*) definíció szerint teszi, amely természetesen az összes, más szubkultúrába tartozó hackerben rossz érzéseket kelt.

Amikor az általános médium a *cracker* szót használja, akkor többnyire ugyanezt érti rajta, ez a megnevezés azonban főleg a hacker definíciójának 1. pontjában található csoport tevékenységének köszönhetően jelent meg a médiában – rengeteg félreértésnek teret adva ezzel, nem beszélve a hackerek 2. csoportjába tartozók tiltakozásáról.

A céges hacker

Az eddig definiált csoportosulásokon kívül említésre méltó még a nagyobb vállalatok és szervezetek által felbérelt hackerek által képviselt közösség, valamint a biztonsági auditorok csoportja.

A hackereknek nevezett csoportok tagjainak többsége a karrierjét egy idő után nagy cégek alkalmazottjaként – technikai szakemberként (behatolástesztet végző, úgynevezett etikus hacker), vagy folyamatokat áttekintő, a rendszerekre és az információbiztonsági kérdésekre nagyobb összefüggésekben tekintő csoport (auditorok, CISM, CISA⁵ vizsgákkal rendelkezők) tagjaiként – folytatja.

Ezek közt a teljesség igénye nélkül léteznek a különböző szervezetek által vizsgáztatott, „papírral rendelkező” csoportok (a technikai területen pl. CEH⁶) és az autodidakta módon képződött,

valódi technikai háttérrel rendelkező hackerek csoportja. Ezek közt nem túl nagy az átfedés. A technikai anyagot és módszereket, amelyeket a hackerek alkalmaznak, el lehet sajátítani, és meg lehet tanulni könyvből, az a gondolkodásmód azonban, amely a hackert hackerré teszi, nem tanulható.

Egy elképzelt beszélgetést bemutatva megláthatjuk, miért van szükség a vállalatoknál a hackerre, és miért a biztonságos rendszer kialakítására és a prevencióra érdemes fókuszálni ahelyett, hogy üldözzük és levadásszuk a hackereket, ezzel látszólag létrehozva a biztonságosabb világot.

Hacker: „Miért csináltuk? Mert meg tudjuk csinálni!”

Manager: „Miért tudjátok megcsinálni?”

Hacker: „Azért, mert hibás a rendszered.”

Manager: „Miért hibás a rendszerem?”

Hacker: „Azért, mert nem figyelsz, benne hagytad a lyukat, és így beengedtél bennünket!”

Manager: „Nem hagyhattam benne a lyukat, mert nem én fejlesztettem a rendszert, csak egy ártatlan áldozat vagyok!”

Hacker: „Ki telepítette a rendszert?”

Manager: „A rendszergazdám.”

Hacker: „Ki választotta a rendszergazdát?”

Manager: „A HR-esem, a humánpolitikai vezetőm.”

Hacker: „Ki választotta a HR-est?”

Manager: „Én.”

Hacker: „Választottál egy HR-est. A HR-esed választott egy rendszergazdát. A rendszergazdád benne hagyta a lyukat a rendszeredben. Neked csinálta, te pedig fizetted érte. Ez ugyanaz, mintha te hagytad volna benne a lyukat.”

Manager: „Hogyan kerüljem el legközelebb az ilyen jellegű incidenst? Másik HR-est válasszak?”

Hacker: „Ne. Inkább lásd be, hogy szükséged van a hackerre. Válassz engem, és megcsinálom neked normálisan a rendszeredet. Nem lesz benne lyuk.”

Így válik sok hacker céges hackerré.

A Valóság

Természetesen a vitázó felek közt nem lehet igazságot tenni, hiszen, mint a viták többségénél, a maga szempontjából minden vitázó félnek igaza van. Egy kritikus paraméter alapján könnyedén különbséget tehetünk a szubkultúrák között: tagjai bűnözők vagy nem bűnözők.

Szubkultúra megnevezése	Szubkultúra leírása	Morális elkötelezettség	
Hacker(1)	Kiemelkedően nagy tudású, elsősorban nyílt forráskódú szoftverekre specializálódott szoftverfejlesztők és rendszer-adminisztrátorok csoportja	Soha nem bűnöző	☀
Hacker(2). Whitehat	Kiemelkedő technikai tudású, elsősorban egy adott operációs rendszer mély szintjeire és hálózati biztonságra specializálódott szoftverfejlesztők és rendszer-adminisztrátorok csoportja	Nem bűnöző, de gyakran van bűnözői múltja	☀
Hacker(2). Blackhat	Kiemelkedő technikai tudású, elsősorban különböző operációs rendszerek mély szintjeire és hálózati biztonságra specializált informatikai szakértők csoportja	Technikailag mindig bűnöző, morális alapon lásd „A hacker valódi motivációja” című fejezetet	⊘
Hacker(2). Greyhat	Kiemelkedő technikai tudású, biztonságra specializált informatikai szakértők, szoftverfejlesztők és rendszer-adminisztrátorok csoportja	Morálisan sem a bűnözői, sem az erkölcsös irányba nem elkötelezett, tudását saját önös céljaira használja	◯
Script kid / wannabe	Csekély technikai tudású, főként 13 és 20 év közötti fiatalemberekből álló szubkultúra, amely a hacker(2) csoport tudására és eszközeire szert téve saját céljai eléréséhez visszaél azokkal	Mindig bűnöző, és a morális hajlam is alapvetően a bűnözők csoportjába helyezi	⊘
Cracker(1). Warez	Szoftvereket a licenszeléstől függetlenül használhatóvá tevő, rendkívül nagy szoftverfejlesztői tudású informatikai szakemberek csoportja	Mindig bűnöző	⊘
Cracker(2). Hacker	A hacker(1) szubkultúra által cinikusan összerosott hacker(2) definíciónak megfelelő informatikai szakemberek csoportosulásainak gyűjtőneve	A rosszindulatú összerosás következményeként bűnözőként szokás értelmezni	⊘

2. táblázat. A hackerek csoportjai

A probléma főként abban rejlik, hogy a média a hackert a crackerrel és a script kiddel összemosva kommunikálja, ezáltal bűnözőkkel azonosítja őket, amit a hacker(1)-ek természetesen kikérnek maguknak, mivel szubkultúrájuk tagjai között egyetlen bűnöző sincs. A hacker(2)-ek viszont morális alapon megkülönböztetik egymást a szubkultúrán belül is, így alakulnak ki a 2. táblázatban található csoportosulások.

Az egyszerűség kedvéért a következőkben a *hacker* szót a hacker(2) definíció Blackhat és Greyhat csoportosulásaira fogjuk érteni, amely csoportosulásokra jellemző a rendkívül nagy technikai tudás, a bűnözői hajlam, és többnyire 16 és 28 év közötti fiatal férfiakat foglalnak magukban.

A világ veszélyei – konkrét célpontok elleni támadások

Az alábbiakban felhívjuk a figyelmet néhány olyan módszerre és technikára, amelyeket a hacker, a hírszerző és a magánnyomozó egyaránt szívesen használ a célszeméllyel kapcsolatos információ megszerzésére. Ezekkel szemben az átlagember is könnyedén megvédeheti magát, ha tudatosan kezeli az információkat, amelyeket megoszt és/vagy megvéd a számítógép-használat során. Bemutatunk olyan módszereket is, amelyek teljes országokkal szemben is hatékonyan használhatók, sőt egyes elemzők szerint a diplomáciai értelemben vett modern háború vagy kiberháború (*cyber warfare*) eszközeinek is tekinthetők.

WIFI

Érdekes problémákat vet fel a WIFI, azaz a vezeték nélküli internet levédése és titkosítása. Közelmúltbeli vizsgálódásaink azt mutatják, hogy tízből két, interneteléréssel rendelkező otthonban a mai napig konfigurálatlan, vagyis alapértelmezett konfigurációs beállításokkal rendelkező WIFI routereket kötnek az ADSL-es

vagy kábeles internetelésre, hogy az elérés így lappal vagy PC-vel kényelmesebbé és kábelmentessé váljon.

Ezt jelenti, hogy a potenciálisan rosszindulatú hackernek semmi más dolga nincs, mint néhány száz métert megtenni autóval a városban, és lappal figyelni az internetelések titkosítási állapotát. Így könnyen megtalálhatók azok a családok, amelyek jelszó nélkül osztják meg a világgal az internetet. Ezekre rácsatlakozva a hacker gyakorlatilag az előfizető – azaz a családtagok – nevében tevékenykedhet az interneten, és ha ezt ügyesen csinálja, akkor tevékenységét szinte a felderíthetetlenségig leplezheti.

Azt gondolnánk, hogy azok a cégek, ahol elméletben szakmailag felkészült rendszergazdák dolgoznak, felelősebben kezelik internet-hozzáférésüket, illetve a belső hálózatukhoz való hozzáféréseket. Védik adatbázisaikat és a dokumentumokat, a cég belső adatait. Természetesen ez szintén tévedés – a mai napig rengeteg cég környékére elég elsétálni egy lappal, és a jelszó nélküli vagy gyenge jelszóval rendelkező WIFI-re csatlakozva már hozzáférést is nyerhetünk a belső hálózat által „rejtett” dokumentumokhoz, belső adatbázisokhoz, meghajtókhoz.

Ezen a ponton fontos kiemelnünk, hogy egy céges WIFI-t semmiképp nem elegendő levédeni egy (akármilyen hosszú) jelszóval, ezek mellé mindig kulcsos azonosítást vagy egyéb többfaktorú, többcsatornás azonosítási módszert kell alkalmaznunk a belső háló védelmére!

IM világ

Egyre jobban elterjedtek az IM, vagyis Instant Messaging protokollok: MSN, ICQ, gtalk és egyéb „chat” felületek, amelyek azonnali üzenetváltási lehetőséget biztosítanak a listáinkon lévő emberekkel.

Sokan használják e felületeket bizalmas vagy akár üzleti jellegű információk továbbítására anélkül, hogy tisztában lennének ennek kockázataival. E felületek közül egyedül a Skype az, ame-

lyik valódi titkosítási lehetőséget biztosít felhasználói számára. Ennél is legalább két paramétert figyelembe kell vennünk a jelenleg publikált információk szerint:

1. Ha a támadó félnek nincs és semmilyen módon nem is volt hozzáférése ahhoz a számítógéphez, amelyiken a beszélgetés történik, akkor a Skype-üzenetváltások nehezen támadhatók. De tudnunk kell: ilyenkor egy nem publikált algoritmust alkalmazunk, amelyhez az amerikai hatóságoknak, és ezeken keresztül – szélsőséges esetekben – valószínűleg a többi hatóságnak is van valamilyen dekódoló algoritmus.

2. Másrészt a Skype-üzenetváltások, amennyiben ezt a funkciót a Skype-programban nem kapcsoljuk ki, szöveges módon rögzítve vannak, tehát a Skype-üzenetváltásaink szöveges részei könnyedén áldozatul eshetnek a potenciális támadónak.

Fontos tudni: az ICQ, MSN, gtalk, Facebook chat és az összes egyéb chat megoldás alapból nem titkosított. Ez annyit jelent, hogy ha a felhasználó akár egy reptéri, akár egy vendéglátó-ipari egységen keresztül, vagy egy otthoni, titkosítással nem védett vezeték nélküli interneten csatlakozik ezekhez a felületekhez, akkor nem csak az itt közvetített információ válhat könnyedén közkinccsé, hanem a felhasználó jelszavai, és a megoldástól függően akár a korábban, jobban védett környezetben folytatott beszélgetései is.

Közösségi portálok

A web 2.0 alkalmazásával 2007 óta számtalan olyan közösségi oldal jött létre, amelyeken a felhasználók profilekat hozhatnak létre maguknak, amelyeken személyes információikat oszthatják meg egymással, és a felhasználók e tartalmak miatt látogatnak oda. (Lásd még Szabó Endre és Talyigás Anikó fejezetét.)

Az ilyen közösségi oldalak a hacker és az üzleti hírszerzésre szakosodott magánnyomozó számára egyaránt kiváló információforrást biztosítanak, hiszen több ilyen oldalról összeollózott

információval, a megbízó által biztosított egyéb információkkal és jól kiválasztott adatbázisokkal, valamint az egyéb kutatási módszerekkel együtt szinte bárkiről bármilyen információt ki lehet deríteni. Mindezt úgy, hogy ezen információk jelentős részét az érintett önszántából osztja meg velünk.

A közösségi portálok használói két fő szempontról megfélekeznek: egyrészt a megosztott információt esetleg nem csak a közösség tagjai láthatják, másrészt a különböző ilyen jellegű portálokon megosztott információk és egyéb helyen elérhető információk együttesen már nem csak az illető személyes adatait, barátait és a kapcsolati körével kapcsolatos egyéb információkat hordozzák magukban, hanem teljes gondolkodásmódját, személyiségprofilját is. Ezeket az információkat összeollózva a felkészült megfigyelő messzemenő következtetéseket vonhat le az illető szokásrendszerével és viselkedési mintáival kapcsolatban. Ezek az információk potenciális támadási felületet jelentenek szinte bárki számára akár személyes, akár szervezeti szinten.

A túlzott megosztási kedvvel (angolul over-sharing) kapcsolatban az a weboldal keltette a legnagyobb visszhangot, amely 2009 végétől 2010 elejéig több mint fél éven keresztül lehetővé tette a közösségi portálokon a felhasználóknak fizikai helyzetük megadását is (lásd kötetünkben Szabó György írását). Az információt a pleaserobme.com weboldal készítői kontextusba helyezték, azaz a helyzetét megosztó illető felhívja a potenciális betörő figyelmét arra, hogy ha nem tartózkodik a lakásában, lehetőség nyílik annak kifosztására.

A szervezett bűnözés és a hackerek kapcsolata

Főként az orosz és a kínai Blackhat-csoportok között találhatók ma már olyanok is, amelyek tagjai elfogadják a szervezett bűnözés által felajánlott busás összegeket, és így bizonyos speciális támadásokat hajtanak végre nagyobb cégek és szervezetek, vagy akár egész országok ellen.

E támadások célja lehet: adott személyes vagy üzleti információ, esetleg a kontroll megszerzése az adatok felett, vagy az adott szervezet informatikai infrastruktúrájára vagy akár *good-willjére*⁸ való csapásmérés, amely adott helyzetben, ahogy azt számos eset is mutatja, csődbe is viheti a céget.

Ilyen jellegű támadásokra sok példa van, gyakran azonban a támadásig a felek el sem jutnak, ugyanis az elsősorban orosz szervezett bűnözés módszere, hogy összefognak a velük együttműködő, megfelelő *packet powerrel*⁹ rendelkező hackerekkel vagy hackerek csoportjaival. A következő lépés, hogy amikor az együttműködés feltételei tisztázottak, a bűnözői csoport egy képviselője kapcsolatba lép a kiszemelt áldozattal (pl. e-bay, amazon,¹⁰ pornóoldalak, online casinók stb.), és védelmi pénzt követel. Egy ekkora internetes vállalkozásnak egy napi *downtime*¹¹ a megfelelő időzítéssel akár több millió dolláros veszteséget is okozhat, ráadásul maga a Distributed Denial of Service¹² támadás effektív technikai kivitelezése a támadó fél részéről gyakorlatilag semmilyen erőfeszítést nem igényel egy parancs kiadásán kívül, és akármeddig, egészen pontosan a támadást leállító parancs kiadásáig fenntartható. Ez azt jelenti, hogy egy ilyen támadás elméletileg akár hetekig is eltarthat. Ha a megtámadott fél – amely lehet nagy tőkével rendelkező üzleti vállalkozás vagy fontos állami intézmény – politikailag is fontos, és megfelelő a felvonultatott hackertámadás, akár háborús eszköznek is tekinthető a nemzetközi diplomácia színterén.

Oroszok és észtek

Ilyen típusú támadásra példa az Észtország ellen 2007 májusában végrehajtott orosz akció, amely megmutatta, hogy a DDoS mint eszköz akár egy teljes ország egész informatikai infrastruktúráját is megbéníthatja mindaddig, amíg azt fenntartják.

Észtország 1,4 millió lakosú állam, ahol jelentős orosz kisebbség él (1940 és 1991 között a Szovjetunió tagállama volt). Az in-

ternet penetrációja és a szolgáltatások használata a társadalomban jelentős (internetes bankolás, szavazás, benzinvásárlás stb.). A lakosság 60%-a napi szintű internetfelhasználó. Észtországnak azonban viszonylag alacsony a nemzetközi sávszélesség-kapacitása, amely természetesen alapvetően elegendő egy ekkora országnak, egy ilyen kaliberű támadás esetén azonban könnyen jelentheti az ország kritikus infrastruktúrájának legszűkebb keresztmetszetét.

2007. április 27-én az észt kormány úgy döntött, hogy a Bronz-katonának nevezett szovjet háborús emlékművet¹³ elköltözteti az észt főváros, Tallinn központjából. Az észtországi orosz nacionalista kisebbség a lépést támadásként értelmezte, így Tallinn utcái két napra megteltek orosz nacionalista tüntetőkkel. A tüntetésnek halálos áldozata is volt, ez azonban még mindig nem tántorította el az észt kormányt a Moszkva által is barátságtalanként értelmezett lépéstől.

Az orosz hackerek első körben az észt külügyminiszter liberális Reform Pártjának honlapját alakították át saját ízlésük szerint. Hamarosan azonban csaknem az összes minisztérium és Észtország jelentősebb és kevésbé jelentős gazdasági szervezetei is áldozatul estek támadásaiknak.

A támadássorozatot az észt védelmi minisztérium az USA ellen történt szeptember 11-i támadásokhoz hasonlította. Ezzel egy időben az orosz parlament alsóházában, a Dumában az egyik orosz politikus az észt kormány lemondását követelte, és az orosz kormány bojkottálta bizonyos nyersanyagok és a személyi közlekedés forgalmát is Tallinn és Szentpétervár között.

Természetesen az internetes támadás mérete felhívta a mód-szerre a nyugati katonai vezetők figyelmét is: az alvilág által használt DDoS módszere ettől kezdve a nemzetközi politika eszköztévé is válhat, hiszen alkalmas az ellenfél megfélemlítésére, elhallgattatására, infrastruktúrájának potenciális kontroll alatt tartására, és a külvilággal való kapcsolattartás megakadályozására – és ezek által rendkívül értékes fegyver lehet egy háború korai szakaszában.

Érdeemes megjegyezni, hogy az észtországi orosz ellenállók, a hazafias érzelmű kisebbség tagjai észt közalkalmazottak e-mail

címét publikálták különböző, mindenki számára elérhető fórumokon, kiszolgáltatta azok tulajdonosait a tettekre kész nacionalisták által pornó- és egyéb lapok segítségével létrehozott spam-áradatnak is.

Természetesen ez a módszer, habár jelentős kellemetlenséget okozhat az észti közigazgatásnak, korántsem jár olyan végzetes következményekkel, mint a DDoS, amelyért a felelősséget az orosz kormány csak két évvel a történetek után, 2009 márciusában ismerte el. Ezt követően már tudjuk, hogy a támadásokat a Kreml-közelitől politológushoz, az Orosz Politikai Kutatóintézet vezetőjéhez, Szergej Markovhoz köthető fiatal emberek egy csoportja követte el.

A támadásokat a hackerek több mint százhusz különböző egyedi célpont ellen indították – egyfelől DDoS botneteket¹⁴ használva, másfelől publikus scriptek¹⁵ (programok) segítségével, amelyeket fórumokon terjesztettek, önálló aktivistákat biztatva, hogy a saját, akár otthoni sávszélességüket arra használják, hogy *ping floodot*¹⁶ indítsanak az észti célpontok ellen.

Ennek hatására az észti CERT¹⁷ és a helyi hatóságok külső segítséggel kezdtek védekezni a DDoS támadás ellen oly módon, hogy a DDoS által telített sávszélességet önként letiltották Észtországban. Ennek köszönhetően bekövetkezett az elkerülhetetlen fordulat: egész Észtországnak ideiglenesen megszűnt a nemzetközi internetelérése, az ország gyakorlatilag leszakadt az internetről.

Kiberhadviselés

A legjelentősebb hatást egy DDoS támadás során a több millió vagy akár több tízmillió, internetes féreggel megfertőzött vagy egy csoportos támadásban feltört számítógépcsoport zombiként való irányítása (botnet) jelenti. Az eredmény: valós felhasználói kérésektől megkülönböztethetetlen, legitimnek tűnő kérésekkel árasztja el az áldozat portálját (informatikai kiszolgálóját), leterhelve ezzel annak számítási kapacitásait, szélsőséges esetben annak sávszélességét is.

Egy DDoS támadás tehát olyan, mintha összeállna tízmillió ember, és egy nagy terhelésre készült weboldalt, amely másodpercenként 5000–8000 kérés megfelelő kiszolgálására van tervezve, a normál kérések mellé elárasztana még másodpercenkénti 20 000 kéréssel. A szerverek számítási kapacitásai és az infrastruktúra sávszélessége is véges erőforrások – és a legitim és illegitim kérések között szinte lehetetlen különbséget tenni.

További érdekesség a sávszélességgel kapcsolatos adatok megfigyelése: 2006-ban a 2–4 gigabit sávszélesség-erősségű (packet power) DDoS támadások voltak az átlagosak és a 8 gigabites támadás már kiemelten erősnek számított. 2009-ben ugyanez a szám 50–60 gigabit. A mértékegység érzékeltetése végett: Magyarország nemzetközi sávszélesség-elérési képessége szakértők becslése szerint 250–300 gigabit méretűre tehető.

Az észet példa nem egyedülálló – a kiberhadviselés hasonló elemei voltak megfigyelhetők 2003 márciusában, az iraki háború kezdetekor, továbbá a dán képregényrajzoló Mohameddel kapcsolatos alkotásainak publikációja után is. Később, 2008 áprilisában politikai okokból támadták meg a CNN.com-ot, 2007 őszén az ukrán köztársasági elnök weboldalát és a Régiók Pártjának weboldalát, 2008 nyarán pedig a NATO weboldalát (feltehetően az ukrán NATO-ellenes tüntetők finanszírozásával), majd a grúz köztársasági elnök weboldalát és a Burma Demokratikus Hangerő nevű újságot is DDoS segítségével.

A hacker pszichológiai profilja

Korábbi definícióknak megfelelően a következőkben a hackeren technikailag rendkívül felkészült informatikai szakemberek olyan csoportosulását értjük, amely bűnözői hajlamú, többnyire 16 és 28 év közötti fiatal férfiakat foglal magában.

E rész célja, hogy bemutassa, kik is a hackerek általában – áttekintjük a hacker pszichológiai profilját és motivációját, hogy elkezdhessünk egy hacker fejével gondolkodni.

A hacker motivációja és társadalmi beágyazódása

De mit is jelent egy hackernél a bűnözői hajlam? E kérdés megválaszolásához érdemes egy kicsit jobban megismerkednünk a hackerekkel és a hackerek motivációjával.

Miért hackel a hacker? A hackerszubkultúrában erre a leginkább elterjedt válasz: „Why? Because we can!” (Lásd a hacker és a manager között lezajlott korábbi párbeszédünket.)

Ez a mondat sokféle értelmezési lehetőséget rejt magában. A külső szemlélő számára könnyen úgy tűnhet, hogy ennek üzenete magyarul – „Miért? Mert megtehetjük!” – a hatalommal való visszaélésre éhes fiatal férfiak csoportja, amely alig várja, hogy megmutassa a világnak, hogy mindenre képes. Azok azonban, akik egy kicsit jobban ismerik a hackerek kultúráját, pontosan tudják, hogy ez a hozzáállás a hackerek többségére egyáltalán nem jellemző, éppen ellenkezőleg: a valódi hackerek többsége szélsőségesen magas intelligenciájú és extrém technikai tudású, de csendes, visszahúzódo személyiség. Általában emellett ők a többség számára kihívást nem jelentő kommunikációs problémákkal küzdenek. A szociális kapcsolatok terén elszigetelődő jellegű személyiségükből fakadóan a világtól elszigetelve, gyakran virtuális valóságban élik életüket, és alakítják személyes kapcsolataikat is. A valódi hackerek zömének többnyire megvan ugyan a maga szociális kapcsolati hálója, ahol elismerik a tudását, és megbecsülik, ez azonban élesen különbözik a fizikai világban megszokottól. A hacker többnyire autodidakta módon szerzi meg tudását, és a hozzá hasonló adottságú személyekkel keresi a többnyire csak kevés valós életbeli fizikai kontaktussal járó kapcsolatot.

Közismert, hogy a 14–19 év közti személyiségfejlődésben az ember gyakran a lázadás korszakát éli meg. Gyakran találkozunk fiatal, lázadó művészek munkáival, akik graffitivel torzítják el a városok épületeinek homlokzatát. Hozzájuk hasonlóan az ebben a korban járó, a fenti adottságokkal rendelkező felnőtt fiatal emberek többsége rendkívüli képességeit és a saját maga által megszerzett extrém technikai tudást – jobb időtöltés híján – eb-

ben az időszakban oly módon használja fel lázadása megélésére, hogy azzal visszaél: hackel.

Ez a visszaélés azonban sokféle lehet – introvertált, befelé forduló személyiség esetén ezt a képességét a további tudás megszerzésére és információszomjúság által vezérelve gyakran arra használja fel, hogy olyan adatokat, adatbázisokat, hozzáféréseket, információkat szerezzen meg, amelyek az átlagpolgár számára elérhetetlenek.

Extrovertált személyiség esetén gyakran dicsekvő vagy megalázó, tipikusan lázadó módon cégek és szervezetek arculatán, weblapján hagyják ott kézjegyüket (*deface*).

A hacker gondolkodásmódja

A hacker személyiségprofiljának rövid felvázolása után talán már tisztábban érzékelhető a „Why? Because we can!” ars poetica mögötti valódi üzenet, amelyben a páváskodó, hatalommal visszaélő, akár szadista diktátorba hajló személyiségtípus helyett a tudást kutató, enyhén cinikus humorral értelmező „Miért? Mert meg tudjuk csinálni!” értelmet nyer. Az értelmezés kedvéért illusztráljuk ezt egy kifejtett párbeszédben a virtuális áldozat és a hacker között.

Hacker: „Miért csináltuk? Mert meg tudjuk csinálni!”

Manager: „Miért tudjátok megcsinálni?”

Hacker: „Azért, mert hibás a rendszered.”

Manager: „Honnan tudod, hogy hibás a rendszerem?”

Hacker: „Onnan, hogy nem létezik tökéletes rendszer, és én pedig a gondolkodásmódomból és a tudásomból eredően minden rendszerben a hibát keresem.”

Manager: „Miért a hibát keresed a rendszerekben?”

Hacker: „Azért, mert ez köt le: mindig azt keresem, hogy mivel tudom lekötni magam, és ez kihívás, és mivel okosabb vagyok, mint a legtöbb ember, aki a rendszereket kitalálta, és mivel biztonsági rendszerekről beszélünk, ezért mindig valami olyan információ a jutalmam a rendszer kijátszásakor, amelyhez amúgy soha senki sem férne hozzá. És én szeretem a titkos dolgokat.”

Manager: „Minden rendszer hibás?”

Hacker: „Logikailag minden zárt rendszeren belül kell hogy található legyen olyan elem, amely az adott rendszeren belül nem értelmezhető, és ezért a rendszerből való kilépési pontot biztosít. Ez lehet emberi hibából eredő értelmezhetetlenség, vagy magának a rendszernek a hibája is, de ez már filozófiai kérdés.”

Konklúzió – a biztonságos rendszer

Biztonságosnak azt a rendszert tekinthetjük, amelynek biztonsága megkerülése vagy kiiktatása nagyobb erőforrás-mennyiséget igényel, mint az általa védett dolog értéke. Feltörhetetlen rendszer nem létezik, pusztán olyan rendszer, amelyet feltörni drágább, mint amekkora a feltöréssel megszerezhető érték.

A rendszer biztonsági szintje, nagyon leegyszerűsítve, a védekezési rendszerek technikai komplexitásától függ. A probléma az, hogy mindig lesz olyan ember, aki egy fokkal nagyobb mélységben látja az összefüggéseket a rendszer komplexitási szintjénél, és ezért egy fokkal tovább lát azon, így képessé válik túllépni rajta, azaz feltörni azt.

Ennek alapján minden rendszer kijátszható. Egy mindenki számára megérthető hasonlattal élve: a biztonságos rendszer létrehozására tett kísérletek és a rendszerek hibáit kihasználó, azok korlátai közül való jogosultságszerző kilépés összefüggésrendszere kísértetiesen hasonlít a világ működésének értelmezését célzó, megdönthetetlen elméletek létrehozására irányuló tudományos törekvése és a számítástechnika fejlődéséhez jelentős mértékben hozzájáruló, Kurt Gödel¹⁸ 1931-es nemteljességi tételének problematikájára. Eszerint: „Ha egy rendszer ellentmondásmentes, nem lehet teljes, ezért minden ellentmondásmentes, formális-axiomatikus elméletben megfogalmazható olyan mondat, mely se nem bizonyítható, se nem cáfolható.”

Az informatikában az alapvető problémák az infrastruktúrában, illetve annak szintjeiben rejlenek. Mindig lesz egy adott szint,

amelyen a rendszer működik, például szoftver fut rajta, és egy „alacsonyabb” szint, például az adathordozó, amely a rendszert tárolja, és amelyet valaki meg tud támadni, és ezért az összes feljebb lévő szinthez hozzáférést szerez. Az adott rendszerből való, nagyobb rendszerbe történő kilépési pont mindig egy ilyen, a Gödel-tételhez hasonló elvi összefüggésrendszer meglátásában, a nem bizonyítható és nem cáfolható állítás megtalálásában rejlik.

A modern biztonságtechnikában már nem az az elsődleges cél, hogy olyan rendszert csináljunk, amelyet nem lehet feltörni, hiszen tudjuk, hogy ez az előző, és többnyire elfogadott érvelés alapján logikai képtelenség. Természetesen ez nem szabad hogy apátiába taszítsa a biztonságért felelős szakembereket. Ezért pontosítva: a feladat az, hogy olyan, elég biztonságos rendszert kell kialakítani mindig az általa védett értéktől függően – mivel feltörhetetlen rendszer nem létezik –, amelyről legalább azt biztosan és időben meg tudjuk állapítani, hogy illetéktelen behatolás történt.

Ez már lényegesen könnyebb feladat.

Az információbiztonsági harcra nincs, és logikailag soha nem lehet végleges megoldás – mindig lesz olyan cég, amely adatai védelmében egyre bonyolultabb biztonsági rendszert fog tervezni, és mindig lesz egy, az adott rendszer „kilépési pontját” megtalálni képes okos gondolkodó, aki hatástalanítani tudja ezt a védelmet.

Bizalmas adataink védelmében javasolt mindig az adott adat értékének és érzékenységének – az esetleges kár értékének, amelyet elszenvedhetünk, ha adataink más kezébe kerülnek – megfelelő védelmi rendszert kialakítani, és ehhez, amennyiben erre valóban szükség van, olyan szakemberek segítségét igénybe venni, akik ismerik a hackerek gondolkodásmódját és módszereit.

Checklist-ajánlás a jelszóminősítéshez

A kedves olvasó a 3. táblázat kérdéseinek segítségével a teljesség igénye nélkül elemezheti az információbiztonsággal kapcsolatos saját gondolkodásmódját és gyakorlati szokásait.

Milyen adatokat tárolok a számítógémemen vagy az e-mail szolgáltatómnál (gmail, freemail stb.), amely értékes lehet, vagy kárt okozhat bárkinek?
Valóban szükséges-e, hogy ezeket az adatokat a számítógémemen vagy e-mail szolgáltatómnál tároljam?
Milyen információkat osztok meg magamról a különböző közösségi portálokon (iWiW, Facebook, Twitter, Xing, LinkedIn, blog stb.)?
Mit lehet rólam kideríteni egy sima kereséssel, milyen találatok vannak rólam a nagyobb keresőkön (Google, Yahoo stb.)?
Van-e fizetős vírusirtó szoftver a számítógémemen? Ha igen, akkor érvényes-e még az előfizetésem, mikori az adatbázisa?
Van-e titkosító szoftver a számítógémemen?
Nyolc vagy több karakteres-e a jelszavam, és szerepel-e benne kisbetű, nagybetű, szám és speciális karakter?
Használok-e e-mailt bizalmas információk továbbítására?
Használok-e mobiltelefont vagy sms-t bizalmas információk továbbítására?
Használok-e valamilyen Instant Messaging (MSN, gtalk, ICQ) megoldást bizalmas információk továbbítására?
Az általános weboldalak elérésére http-t vagy https-t használok-e, amikor mindkettőre lehetőség van?
Frissítem-e számítógémem operációs rendszerét rendszeresen (pl. Windows update)?
Van-e otthon WIFI (vezeték nélküli internet), és ha igen, akkor le van-e titkosítva legalább egy jelszóval?

3. táblázat. Ellenőrző kérdések a biztonságos internethasználattal kapcsolatban

Székely Iván

Társadalmi informatikus, az adatvédelem és az információszabadság multidiszciplináris területeinek nemzetközileg ismert szakértője és kutatója, az OSA Archivum főtanácsadója, a BME docense

KUKKOLÓ TÁRSADALOM – AVAGY VAN-E MÉG FÜGGÖNY VIRTUÁLIS ABLAKUNKON?

Ha valaki harminc évvel ezelőtt egy nyugati demokráciában azt jósolta volna, hogy 2010-re minden lépésünket kamera követi és ellenőrzi, ezt mindenki elképzelhetetlennek tartotta volna egy szabad országban. Ha valaki 1990-ben azt jósolta volna, hogy húsz év múlva minden üzenetváltásunkat és telefonkapcsolatunkat rögzítik és elemzik, ez legfeljebb a rendszerváltó országok rémálmaiban jött volna elő. Ha pedig valaki csak 2005-ben azt jósolta volna, hogy a házunk kertjében zajló események az interneten bárki számára láthatóvá válnak, Huxley *Szép új világa*,¹ Orwell Nagy Testvére,² esetleg Warren és Brandeis 1890-es híres tanulmánya³ juthatott volna eszünkbe.

Ez a világ pedig eljött. Nevet is kapott a társadalomtudósoktól: *Surveillance society*, azaz megfigyelési társadalom, vagy kényszerlenebbül: kukkoló társadalom.

Az alábbiakban azt próbáljuk körbejárni, milyen okai és következményei vannak a kukkoló társadalom kialakulásának, milyen érvek szólnak a megfigyelés mellett és ellen, milyen válaszok születtek eddig erre a helyzetre, illetve hogy hogyan is élhetünk együtt ezzel a jelenséggel, az információs társadalom e sajátosságával.

Ki figyel meg kit?

Először is – mit nevezünk „megfigyelésnek”? Megfigyelni sok mindent lehet, sokféleképpen: megfigyelhetünk természeti eseményeket, technológiai folyamatokat, forgalmi helyzetet, helyszínt, eseményeket – és embereket, mégpedig arctalan tömegként és azonosítható egyénenként egyaránt. Társadalomképünk szempontjából ez utóbbi a lényeges, ezért vizsgálódásunkat is e területre összpontosítjuk. Még itt is megszorítást kell tennünk: a megfigyelés nem egyenlő az észleléssel. Ha valakit felismerünk az utcán, vagy észleljük tevékenységét, az nem okvetlenül jelenti az illető „megfigyelését”. Az átláthatóság sem egyenlő a megfigyeléssel: ha minden fél tudatában van annak, hogy jelenléte, tevékenysége közösen elfogadott szabályok alapján a többiek előtt zajlik, nem beszélhetünk megfigyelésről. A nyilvánosság sem egyenlő a megfigyeléssel: ha valaki közszereplést végez, és a tüntetésen szónokol, akkor a közönsége azzal, hogy meghallgatja, amit mond, nem tartja őt megfigyelés alatt.

Mi minősül tehát megfigyelésnek (*surveillance*)? Abban a legtöbb meghatározás megegyezik, hogy emberek viselkedésének, tevékenységének többnyire ismételt vagy rendszeres monitorozásáról van szó. Megfigyelésen azonban nemcsak vizuális megfigyelést értünk: egy beszélgetés kihallgatása, a kommunikációs kapcsolatrendszer feltérképezése, e-mailek jogosulatlan elolvasása, telefonbeszélgetések lehallgatása, a térbeli mozgás követése mind-mind a megfigyelés területei. A szinkronitás, a valósidejűség sem feltétele a megfigyelésnek. Ha egy kamera felvételét csak később nézik vissza, vagy egy e-mailek kommunikáció tar-

talmát csak később elemzik, attól még az érintett személyek megfigyelése és a megfigyelés során gyűjtött adatok felhasználása történik. Sőt megfigyelés történhet utólag is, az archív adatok elemzésével, adattárházak építésével, adatbányászati módszerek alkalmazásával.

Egyesek megkülönböztetik a megfigyelést a profilírozástól, vagyis attól a tevékenységtől, amelynek során a megfigyelt személy adatai automatikusan gyűlnek, és építik például internetes vásárlási profilját, politikai színeképét, társadalmi (vélt vagy valós) devianciáját. Mások – elsősorban az angol szakirodalomban – külön kifejezést használnak az emberek adataikon keresztüli megfigyelésére: *dataveillance*. Ismét mások a megfigyelés sajátos területének tartják a repülőtereken alkalmazott – megszegényítő – tesztkennert, amely természetesen nemcsak az utas által hordott fegyver, robbanóeszköz esetleges jelenlétéről ad információt.

Talán a megfigyelés három legfontosabb attribútuma: az információs aszimmetria, az aktus rejtettsége, valamint nem kontrollálható volta.

- Az első, az információs aszimmetria abból adódik, hogy a megfigyelő fél többet tud a megfigyeltről, mint fordítva, és eszközei is jelentősen erősebbek a másikéinál. Mondhatjuk: a megfigyelt fél az esetek döntő részében gyanútlan.

- A második jellemző, az aktus rejtettsége nem okvetlenül a megfigyelés titkos, észlelhetetlen jellegéből adódik, hanem abból is, hogy a megfigyelés eredményeképpen született adatok sorsa – például hogy ki fér az adatokhoz, azokból milyen következtetést von le, azokat mikor, milyen célból fogja felhasználni – az érintett számára nem átlátható.

- A harmadik attribútum, a kontrollálhatatlanság pedig azt jelenti, hogy gyakran még tiltakozni sem lehet a megfigyelés ellen, azt nem lehet kikerülni, az adatok sorsát pedig az érintett személy nem, vagy csak alig tudja befolyásolni.

Ilyen megfigyelés mindig is volt az emberi társadalmak történetében; voltak titkos ügynökök, titkosszolgálatok, kíváncsi szomszédok és kíváncsi hivatalnokok – diktatúrákban több, de-

mokratikus jogállamokban kevesebb. Eddig azonban a megfigyelés volt a kivétel, a „megfigyeletlenség” a fő szabály.

A magyar olvasó, nem is indokolatlanul, úgy érezheti, hogy az elmúlt politikai rendszerben – főként annak korai szakaszában – úgyszintén a megfigyelés volt a fő szabály, a rendszer mindenkit ellenőrzött. Gondolhatunk itt a III/III-as csoportfőnökségtől a KGB-n át a Stasi⁴ kiterjedt besúgóhálózatára, a belügyi alkalmazásban álló házmesterekre, a jelentésekre, telefonlehallgatásokra, levélfelbontásokra. Azonban ez a megfigyelés, bármilyen kiterjedt volt és bármilyen súlyos következményekkel járt is, nagyságrendjében és univerzalitásában nem hasonlítható a mai kukkoló társadalom mindennapjaihoz. Ráadásul a megfigyelés állami monopólium volt, ma pedig e monopólium egyenrangú részese az üzleti szektor, önállóan és az állammal összefonódva egyaránt, és egyre inkább részt kaphat belőle bárki, aki másokat meg akar figyelni vagy figyeltetni. Egyetlen Nagy Testvér helyett számos Kis Testvér és Unokatestvér dolgozik már a kamerák mögött, a számítógépközpontokban és az interneten.

Mit sért a megfigyelés?

Amit a megfigyelők megsérteneek tevékenységükkel ma is, és megsértettek a múltban is, az a magánszféra, angolból átvett kifejezéssel a *privacy*. Hogy mi is a *privacy* valójában, erről könyvtárnyi definíció, elemzés született, és születik még ma is. Ismeretes, hogy a fogalom jelentése jóval szélesebb, mint amit a magyarban a jobb híján használt „magánélet” lefed: nem a személyes intimitásokról, nem „az egyedülléthez való jogról” van szó csupán, hanem a magánszféra egésze feletti rendelkezésről.

Ha megnézzük a *privacy* fogalmának történelmi fejlődését az elmúlt évszázadban, még az angol nyelvterületen belül is két tendenciát láthatunk:

– egyfelől erősödik az információs elem jelentősége⁵ (már nem csak a magánlakás, a fizikai magánélet sérthetetlenségét jelenti),

– másfelől egy hagyományos védelmi koncepció felől egyre inkább egy aktív, önrendelkezésen alapuló irányzat felé mozdul el.

Ez utóbbi Magyarországon – a német modellt követő országokhoz hasonlóan – különösen érzékelhető, hiszen a Harmadik Köztársaság alkotmánya és az azt kifejtő Alkotmánybíróság szerint fő szabályként mindenki maga rendelkezik a róla szóló információk sorsáról (lásd Szabó Endre fejezetét).

Természetesen mások a magánszféra határai egy faluközösségben, egy lakótelepen, egy munkahelyen, egy baráti közösségben, és mások voltak évtizedekkel ezelőtt, mint ma. Ha a privacy határait pontosan nem is tudjuk meghatározni, annyit leszögezhetünk, hogy kulturális értelemben nyugati társadalmi fejleményről, mégpedig modern, a fejlett nyugati társadalmakra jellemző fejleményről van szó. Ez a fejlemény szorosan összefügg a nyugati kultúra fejlődésének alapvető elemével: az egyén, az individuum fontosságával. Az egyén és az egyéniség fontos, az egyén nem olvad bele az arctalan tömegbe, vannak saját javai, fizikai és szellemi magántulajdona, és vannak ezzel kapcsolatos jogai és igényei. Tévedés lenne azt hinni, hogy ez az igény csak a gazdag országok gazdag polgárainak luxusa: egy szegény angol család ugyanolyan büszke magánéletének határait, mint ahogy egy szicíliai ház falai mögött történetek sem tartoznak a külvilágra. Természetesen vannak nincstelen tömegek is, olyan emberek, akiknek sem fizikai, sem szellemi tulajdonuk nincs, legfeljebb belső tartásuk.

Érdemes beszélni a Kelet lakóiról. Keleten ugyanis más az egyén szerepe, a környezet nem a többiek közül kiemelkedőket, a zseniket, a szokatlan, újszerű viselkedést honorálja, hanem a közösség tagjaival való együttműködési készséget. Ugyanakkor tévedés lenne azt hinni, hogy Keleten nem fontos az egyéniség, a magánszféra. Egy Japánban tanuló magyar diák – Vincze Batrix – érdekes tanulmánya számos példát mutat arra, hogy a japán kultúrában milyen fontos szerepet játszik a személyiség védelme, és ez hogyan tükröződik a japán felhasználók internet-használati sajátosságaiban, így a szigorú anonimitás körülményei

között folytatott önfeltárás és a „bensőséges ismeretlenekkel” folytatott kommunikáció elterjedtségében.

A társadalmi fejlődés és az értékrend alakulását a jog is követte. Noha az első modern adatvédelmi⁶ törvény csak 1970-ben született meg a németországi Hessen tartományban, a jogfejlődés hosszú, szerves folyamatát láthatjuk a Habeas Corpus elvétől a mai latin-amerikai alkotmányok Habeas Data fogalmáig.⁷ A szabad ember saját testével való rendelkezésének alapelve (még ha eredetileg csak az indokolatlan fizikai fogvatartás korlátozása volt is a célja) a modern világban kiterjedt a szabad ember saját magáról szóló információival való rendelkezés területére is. Éppen ez az, aminek érvényesítését megnehezíti, gyakran lehetetlenné teszi a mai kukkoló társadalom, és különösen az internetes kommunikáció gyakorlata.

Vajon miért hiányos, korlátozott jelentésű a privacy fogalma a magyar nyelvben, miért nincs rá megfelelő szavunk? Valószínűleg azért, mert a magyar társadalom a II. világháború előtt még(!) nem juthatott el arra a fejlődési fokra, amikor a magánszféra feletti önrendelkezés tömeges igényné, értékké, esetleg tételes joggá vált volna. A világháborút követő évtizedekben pedig már(!) nem volt alkalom arra, hogy a nyugati demokráciák értékrendjét átvegye és szervesen magába olvassza az ország társadalma. Számunkra csak a rendszerváltás után jött el az a pillanat, amikor a megkésett fejlődés egyik állomásaként ezek az értékek és jogok is bekerültek az új alkotmányos jogállam portfóliójába. Ahhoz, hogy e fogalom és tartalma mindennapi életünk természetes részévé váljon, hosszú és kiegyensúlyozott társadalmi fejlődésre lenne szükség; ebben pedig igencsak hiányt szenvedtünk a rendszerváltást követő két évtizedben.

A technológia szerepe és a magánszféra

A mindenkori korszerű információs-kommunikációs technológia azonban kikezdte, erodálta a magánszféra értékének, és egyben a jognak a gyakorlati érvényesíthetőségét. Hiába látjuk a jogfejlődés

ívét a testtel való rendelkezéstől az információval való rendelkezé-
sig, hiába van hatályban a világ több mint hetvenöt országában⁸
a személyes adatok védelmére, a velük való önrendelkezésre vo-
natkozó törvény, és hiába születnek nemzetközi egyezmények és
direktívák arról, hogy miként szabad felhasználni a személyes ada-
tokat, a gyakorlatban nem fejlődést, hanem visszafejlődést látunk,
vagy másképpen: omlások sorozatát. E sorozatban meghatározó
szerepet játszott és játszik a mindenkori korszerű technológia.

Az első nagyobb ilyen omlást a modern nyugati társadalmak-
ban nem az internet, még csak nem is a számítógépek okozták,
hanem a telefónia. A XIX. század közepén az amerikai nagyváro-
sokban mindenki számára világosak voltak a magánélet határai:
ezek egybeestek a birtok, a ház, a lakás fizikai határaival. Ami ezen
belül történt, magánügy volt. Az az érpár, amely bevezette a ma-
gánterületre a telefont, egy csapásra megváltoztatta a helyzetet:
akármilyen kényelmessé és hatékonná tette is a távollévők kö-
zötti kapcsolatot, a magánszférában elhangzottak magánjellegét
többé nem lehetett garantálni. A lehallgatás lehetőségét nemcsak
a telefonbeszélgetések megcsapolhatósága jelentette (ami nem-
csak a központban, hanem a vezeték teljes útvonala mentén le-
hetséges volt), hanem az is, hogy a telefonkészülék egyik fő eleme,
a mikrofon önálló karriert kezdett, és ezzel kialakult a vezetékes
„poloskák” első generációja.⁹ A fejlődés nem volt egyformán gyors
a világ más régióiban, mégis a következő generációk a Föld szin-
te minden pontján már alkalmazkodtak ehhez a helyzethez, meg-
tanulták, hogy mi az, ami „nem telefontéma”.

Az első omlás kulcsmozzanata az információszerzés techni-
kájának forradalmi változása volt, a másodiké az információfel-
dolgozása. Az első nagyszámítógépek megjelenéséről van szó:
amikor a gépek már nem kizárólag ballisztikus röppályák és más
hadi feladatok kiszámításával voltak elfoglalva, a hivatalnokok
hamar rájöttek, hogy segítségükkel az egyes állampolgárokat mi-
lyen hatékonyan lehet nyilvántartani származásuk, vagyoni hely-
zetük, tevékenységük és számos más ismerv alapján. Az 1950–
1960-as évek után felnövő nemzedékek ehhez is hozzászoktak,

de ez az alkalmazkodás már nem volt olyan teljes körű, mint a telefon esetében: még a fejlett országokban is élnek néprétegek, amelyek tagjai ma sem értik teljesen – és többeket még csak nem is foglalkoztat –, hogy tulajdonképpen mi is történik adataikkal a számítógépben és a hálózaton.

A magánszféra értékeinek és jogának érvényesíthetőségében a harmadik, ma is tartó omlási szakasz az internethasználat elterjedése, az „összehuzalozott társadalom” kialakulása. Ennek működését látszólag minden fiatal természetesnek veszi, de azok aránya, akik átlátják és befolyásolni tudják adataik sorsát, egyre kisebb. Most már az információszerzés és -feldolgozás mozzanata szétválaszthatatlanul összefonódik. Egy egérkattintás nemcsak információt szolgáltat egy megfigyelőautomatának, hanem ezt az elemi információt egyidejűleg elemzik is, és továbbbépítik a felhasználó profilját, amihez az érintettnek nincs hozzáférése, befolyása, sőt amiről legtöbbször tudomása sincs.

Mostanra világossá vált, hogy hiába vannak szép elveink, értékeink, jogi garanciáink, a törvényt a „kód” írja, ahogy Lessig elhíresült könyvéből (*Code and Other Laws of Cyberspace*) is tudhatjuk. Ráadásul arra is rá kell eszmélnünk, hogy életünk alakulása egyre inkább attól függ, hogy hol és mit tárolnak rólunk. „Információs hasonmásunk”, „digitális énünk” fontosabbá válik, mint valós személyiségünk. Ebben a helyzetben tehát adjuk át a „törvényhozást”, a szabályok meghatározását az informatikusoknak és megrendelőiknek?

A mai helyzet, avagy a Panoptikontól a Kriptikonig és a Periptikonig

Egy adatvédelmi tudatosságot fokozó projekt háttéranyagából idézünk:¹⁰

„Tudta-e...

– hogy a weblapokon webpoloskák vannak, amelyek megfigyelik, hogy mikor mit néz?

- hogy böngészési szokásaitól függően más hirdetések jelenhetnek meg a képernyőjén, mint másén?
- hogy elemzik, mennyire hajlandó vásárolni, és ezért más-más árat fizethet az interneten?
- hogy ha »értéktelen« ügyfél, akkor sosem juthat élő ügyfélszolgálatoshoz, hanem hallgathatja az automatát?
- hogy az összes e-mailes és mobiltelefonos kapcsolatát legalább fél évig rögzíti a szolgáltatója?
- hogy a Google minden e-mailjét, dokumentumát, fényképét, videóját elemzi?
- hogy a mobiltelefonok, a műholdak, és már a Google is pontosan követik, hol, kivel jár éppen?
- hogy az élete már valójában attól függ, hogy mi van Önről »a gépben«?
- hogy az ingyenes szolgáltatások ára az Ön személyiségének eladása?
- hogy ha nem figyel oda, végképp kicsúszik kezéből a sorsa, karrierje, kapcsolatai irányítása?"

Noha ezek a költői kérdések az átlag internethasználó figyelmének felkeltésére szolgálnak, azért nem kell szakembernek lennünk ahhoz, hogy felismerjük:

- a Google StreetView rendszere nemcsak az utcánkról, hanem a házunkról, az autónkról, az utcán lévő emberekről is felvételeket készít. (A tiltakozások hatására utólag igyekeznek az interneten elérhető változatban kitakarni az emberek arcát és az autók rendszámát).

- A Latitude (People Tracker) követi térbeli mozgásunkat, és fogyasztói profilunkat már a tartózkodási szokásainkkal is összeköti.

- Az egyre több helyen jelen lévő és egyre kevésbé látható kamerák gyakorlatilag titkos megfigyelést végeznek, és az automatikus arcfelismerő rendszerek segítségével a tömegből is kiszűrhetővé teszik az egyént.

- Kommunikációs hálónkat nemcsak a nyomozó szervek, hanem a szolgáltatók és a marketerek is elemzik; számítógépeink-

re spyware-ek, azaz kémprogramok települnek, amelyek megbízók számára továbbítják winchesterünk tartalmát és digitális tevékenységünk jellemzőit.

– A portálok webpoloskákat alkalmazhatnak arra, hogy illetéktelen harmadik felek a tudtunk nélkül monitorozhassák azt, hogy mit nézünk a weben.

Hosszan sorolhatnánk a korszerű megfigyelés eszköztárát.

Jeremy Bentham¹¹ 1780-as években tervezett Panoptikonja avagy „felügyelőháza”¹² egy másik filozófus, Michel Foucault¹³ munkássága nyomán vált a megfigyelő állam közismert metaforájává. Ebben a rendszerben mindenkinek azt kellett éreznie, hogy egy központi helyről megfigyelik, és ezért ehhez kellett igazítania viselkedését. Ma inkább a Kriptikon, vagyis a titkos megfigyelőrendszer lehetne a legjobb metafora: sok helyről figyelnek, és nem látjuk, kik és mikor. És megjelent egy új jelenség is az interneten, amelyet egyes szerzők a „Periptikon” metaforával illetnek – sokan saját akaratukból vetik alá magukat a megfigyelésnek, ha nem is mindig a következmények teljes tudatában (lásd Szabó Endre és Rácz Bencze írásait kötetünkben). Exhibicionisták persze mindig is voltak, de itt másról van szó: a közösségi hálózatokban való részvétel ma kikerülhetetlen elvárás a fiatal generáció tagjai számára. Életüket a Facebookon vagy más szolgáltatásokon kell élniük. Ha valaki ezer internetes „barátot” tud felmutatni, ez vetekszik a divatmárkás cikkek birtoklásának csoporton belüli státusával, míg aki csak ötvenet, azt szinte már ki-közösíti a csoport. Ugyanakkor a résztvevők nemcsak más egyének, hanem intézmények figyelmét is magukra akarják irányítani ezekben a rendszerekben, a társadalmi integráció egyik alapvető formájaként. Ennek egy sajátos formája, amikor a politikusok is ezt a fórumot használják az őket támogató közösség szervezésére. De ők egyrészt közszereplők, másrészt tudatosan használják ezt az eszközt, személyes adataikból szinte semmit nem közölnek.

A „káros mellékhatások” mindennapi életünkben

A korszerű infokommunikációs technológiák (IKT), az internetes világ megannyi áldásos hatásáról sokat hallunk – munkavégzésünk, tájékozódásunk, kapcsolattartásunk, tanulásunk, ügyintézésünk szerves részévé lettek –, ugyanakkor alig ismerjük árnyoldalaikat. Néhány, a megfigyeltségből eredő negatív következményt említünk – negatívak olyan értelemben, hogy a megfigyelt, elemzett és befolyásolt személy számára előnytelen vagy káros a következmény. Természetesen mindig vannak más haszonélvezői e tevékenységeknek. Előrebocsátjuk: ezeket a negatív következményeket nem egyszerűen mellékhatásoknak, hanem a mai kukkoló társadalom technológiájából és működéséből következő alapvető hatásoknak tartjuk.

Képzeljük el, hogy bemegyünk egy vendéglőbe, ahol nincs kihelyezve a bejárat elé az étlap, és ha nagyon éhesnek látszunk, a pincér olyan menükártyát hoz, amelyen magasabbak az árak, hiszen úgyis rendelni fogunk valamit. Ez a helyzet, amelyet joggal kifogásolnánk a vendéglőben, könnyen megvalósítható az interneten. Bizalomgerjesztő neve is van: dinamikus árazás. Internethasználati, fogyasztói profilunk ismerete esetén ugyanis könnyen megbecsülhető, mennyit vagyunk hajlandók fizetni egy termékért vagy szolgáltatásért. Ha a szolgáltató célja egyedül az, hogy minél többet fizessünk, akkor az a legmagasabb ár fog megjelenni a képernyőnkön, amennyire fizetőképesnek tartanak. A szomszédunk képernyőjén lehet, hogy más ár jelenik meg – a lényeg az, hogy nem egyenlő eséllyel indulunk a vásárlásban, és ez a diszkrimináció egyik formája.

Egy másik tömeges jelenség (igaz, hogy nem legális – de hát a kód írja a törvényt, ugyebár) az identitáslopás. Nem hamis identitásokról, hamis virtuális személyazonosító iratokról van szó, hanem valódi, összetartozó adatokról, például névről, lakcímről, társadalombiztosítási számról és bankkártyaszámról. Ezek olyan adatok, amelyekkel vásárolni lehet, tranzakciókat indítani, publikálni – csak éppen mindezt identitáslopás esetén az

érintett tudta nélkül. Ilyen összetartozó identitásokat az internetes megfigyelés robotjai gyűjtenek fáradhatatlanul, és az ilyen felhasználásban érdekeltek olcsón és tömegesen juthatnak használatukhoz.

A *social sorting* vagy társadalmi osztályozás ugyancsak bizalomgerjesztően hangzó fogalom, holott nem más, mint a megfigyelő tevékenység társadalmilag gyakran káros következménye. Képzeljük el, hogy egy bevásárlóközpont vezetőségének nem tetszenek azok a látogatók, akik nem illenek a steril gránit-üveg-acél környezetbe, és abba az életformába, ahol a család programjának napi kulturális csúcspontja a pénzköltés. Ezek az emberek lehetnek színes bőrűek, túl hosszú – vagy éppen túl rövid – hajúak, másként öltözködők, baseball-sapkát viselők, vagy csak túl hangosan sír a gyerekük, és zavarja a bevásárlóközpont hangulatát. Hála a jó felbontású videokameráknak, az automatikus arcfelismerő rendszereknek és a rádiótelefonoknak, könnyen mozgósíthatók a biztonsági őrök, hogy a nemkívánatos személyeket távol tartsák a vásárlóközönségtől – vagyis ismét a diszkrimináció veszélyét látjuk.

Hasonlóan diszkriminatív lehet a szolgáltatásoknak az „ügyfélértékhez” való igazítása – ismét egy vonzóan hangzó elképzelés az üzleti tervek készítőinek, és ismét egy rejtett diszkriminációt hordozó technológia a felhasználóknak. Hogyan lehet az, hogy a kisnyugdíjas sohasem jut élő call centeres munkatárszohoz, az automata mindig visszadobja („ha legújabb ajánlatainkat kívánja meghallgatni, nyomja meg az 1-es gombot”), míg a jó módú szomszéd egyenesen az ügyfélszolgálatos kisasszonyhoz kerül? Úgy, hogy a rendszer az adatok összekapcsolásával tudja, hogy a jó módú szomszéd sokkal több hasznot hoz a cégnek, mint a kisnyugdíjas, a kisasszony órábéra pedig drága.

Említenünk kell a kéretlen e-mailek, a spamek tömegét, ami egyes számítások szerint ma már az e-mail forgalom több mint kilencven százalékát teszi ki, és amelyekben hol orgazmusfokozó szereket, hol nigériai nagybácsi vagyonának kimentését, hol kéretlen szolgáltatásokat ajánlanak. E-mail címünk, kapcsolati part-

nerünk, böngészési és vásárlási szokásaink, tartózkodási helyünk – amelyeken e kéretlen üzenetek generálása alapul – természetesen a tudtunk és beleegyezésünk nélküli megfigyelés és adatgyűjtés útján kerül a spamrobotok és gazdáik birtokába.

Az elmondottak alapján hol vagyunk tehát attól, hogy ebben az internetes világban magunk dönthessünk a rólunk szóló adatok sorsáról? De nemcsak rólunk mint egyénekről van szó: vannak az internetes megfigyelési, adatelemzési és felhasználási technikának olyan negatív hatásai is, amelyek nem közvetlenül az egyént, hanem a társadalom nagyobb rendszereit érintik. Ilyen például a hatalmi viszonyok megváltozása, a személyes autonómia beszűkülése. Az információval bíró (megfigyelő) fél befolyásolási képessége megnő, így a gazdasági és társadalmi folyamatokat, beleértve az egyéni életviszonyok alakulását, nem autonóm polgárok és az általuk választott, átlátható és elszámoltatható intézmények határozzák meg – ahogy azt a nyugati demokráciák ideáljaként ismerjük –, hanem az információs monopóliumok, illetve általánosságban az információs – adatvagyon – szempontból erősebb felek. Ilyen makroszintű hatás a piac torzulása is: amikor a piaci folyamatokat nem a kereslet és a kínálat egyensúlya vezérli, hanem például a dinamikus árazás és más, a vevő megfigyelésén alapuló technikák. Ekkor a piaci folyamatok kontrollálhatósága csökken, s ennek jelentőségét a 2009–2010. évi pénzügyi válságban, illetve az azt követő időszakban nem kell külön hangsúlyozni.

Vajon miért nem hallunk többet ezekről a negatív hatásokról? És itt ne a „veszélydiskurzusokra” gondoljunk (lásd kötetünkben Z. Karvalics László írását), amelyek az internet „veszélyeire” figyelmeztetnek, hanem a reális értékelésre. Vizsgáljuk meg, hogy mennyiben vagyunk még urai saját döntéseinknek a hálózati világban. Miért van az, hogy mindig csak e-demokráciáról hallunk, és sohasem e-diktatúráról? Az e-demokrácia jó dolog, a demokrácia érvényesítésének megkönnyítése, de az e-technológia diktatórikus rendszerek kiszolgálására is alkalmas. Az e-kereskedelem is jó dolog, de nemcsak a tisztességes kereskedelem érvényesülését segítheti elő, hanem az e-kizsákmányolás elterjedését is.¹⁴

Okok és érdekek

Az okok között első helyen kell említenuünk magát a technológiát, amely egyáltalán lehetővé teszi az ilyen kiterjedésű és mértékű megfigyelést, adatelemzést. Tévedés lenne azonban azt hinnünk, hogy csak a technológia ébresztette fel a megfigyelők vágyait, azok megvoltak korábban is. Most viszont létrejött egy szimbiózis, amelyben a megfigyelők újabb és újabb feladatokat adnak a technológusoknak, és e feladatokat a mai technikai, alkalmazási túlkínálatban nem nehéz megoldani műszakilag.

Az üzleti érdekek szerepét sem lehet eléggé túlhangsúlyozni. Az elektronikus kereskedelem és a tartalomszolgáltatás világában már maga az üzleti modell is gyakran eleve a fogyasztó tudta és beleegezése nélküli megfigyelésére, profilírozására, adatainak felhasználására épül, vagyis eleve jogellenes és értéktelen alapokon nyugszik. Ezzel szembe kell néznünk, még mielőtt a naiv felhasználók tömegével együtt azt hinnénk, hogy az „internet” és az interneten elérhető szolgáltatások voltaképpen jótékony szervezetek akciói, amelyek egyetlen célja a felhasználó lehetőleg ingyenes kiszolgálása. Sokan jelezték például már akkor, amikor a spam még nem volt ilyen elterjedt, hogy megfelelő szabályozással, szankcionálással, sőt technikai megoldásokkal korlátozni lehetett volna elterjedését, de az üzleti lobb hatására ezekből a korlátozásokból mindaddig semmi sem lett, amíg a belpolitikai érdekek meg nem változtak.¹⁵

A nagypolitika mellett a közigazgatás érdekei is nyilvánvalóak a megfigyelő társadalom kialakulásában. Az igazgatás mindig is törekedett arra, hogy minél több információt szerezzen a polgárokról, és ezzel jól irányítható közösségeket igazgasson. Ennek számos célja lehet, a sokat hangsúlyozott jóléti szolgáltatások célzottabb nyújtásától a polgárok ellenőrzésén át a közigazgatás saját fontosságának növeléséig és az „igazgatandó” társadalom víziójának megvalósításáig.

Külön említést érdemel a kockázatipar és a politika, illetve a közgazdaság közös érdekszférája. A kockázatipar (angolul *risk industry*), amelyet képviselői jobban szeretnek „biztonságiparnak” nevezni, globális üzletággá nőtt, amely a nemzetbiztonságtól a terrorizmus veszélyén át egészen az egyéni „biztonság” szférájáig minden területet átfog. Mivel a megfigyelési technológiák alkalmazásának egyik fő érve a biztonsági kockázatok csökkentése, a kockázatipar vállalatai pedig profitra törekvő vállalatok, nem nehéz felfedeznünk, hogy alapvető üzleti érdekük a kockázat és az attól való félelem minél magasabb szinten tartása.

Ez egyben a politikusok érdeke is lehet, hiszen ők azok, akik majd garantálják választóik biztonságát, és ebben természetes szövetségeik a megfigyelési technológiákat árusító cégek. Hiába mutatják ki a sokáig titkolt elemzések, hogy még Nagy-Britanniában, a világ legsűrűbben bekamerázott országában sem mutatható ki egyértelműen a bűnözés csökkenése és a kamerás megfigyelés közötti összefüggés¹⁶ (hogy a költség–haszon mutatókat ne is említjük), melyik politikus merne akár csak egyetlen kamerát is leszereltetni – hátha éppen azért történik majd valamilyen bűncselekmény. A kritikusok azt állítják, hogy a bűnözési hajlam a megfigyelés eredményeképpen nem csökken, csak más szelepeken át manifesztálódik, és a politikusoknak és tanácsadóiknak inkább azzal kellene törődniük, hogy mi okozza a devianciát és a bűnözési hajlamot, és ennek okait kellene kezelniük. Ha a bűnözés kizso-
rul a kamerák látóteréből, akkor megjelenik a kapualjakban (rendben, akkor azokat is bekamerázzuk), onnan átkerül a magánlakásokba (akkor a lakásokat is bekamerázzuk), onnan a hálósobákba (nem probléma, a hálósobákat és a mellékhelyiségeket is bekamerázzuk) – ugye nem ilyen információs társadalmat képzelünk el?

A fentiekkel szorosan összefüggő ok az úgynevezett aktuárius társadalom víziójának kialakulása és gyakorlati megvalósulása. Az aktuáriusok, akikről ez a társadalomkép a nevét kapta, a biztosításmatematikások, akik a kockázatokat számolják a biztosítótársaságoknál. Az aktuárius társadalom lényegi eleme az „új büntetéstán”, amelynek számára érdektelen a normalitás és a de-

viancia kérdése, érdektelen a bűnözés és a bűn összefüggése, és érdektelen a megbűnhődött egyén rehabilitálása, visszavezetése a társadalomba – számára csak egy dolog fontos: a statisztikai valószínűség.¹⁷ Eszerint a társadalom minden tagja potenciális bűnöző, terrorista, adócsaló, zsebtolvaj; és nem holmi erkölcsi megfontolások, kulturális és gazdasági körülmények határozzák meg, hogy elkövet-e valamit, amit valaki büntetendőnek ítél, hanem kizárólag a lebukás valószínűsége. Ha a lebukási valószínűség magas, akkor nem fogunk bankot rabolni, ha alacsony, akkor akár robbanthatunk is. A valószínűséget pedig úgy lehet magasan tartani, ha mindenkit állandóan megfigyelés alatt tartunk. Azt, hogy mit kell devianciának vagy büntettnek tartanunk, majd megmondja a megfigyelő vagy megrendelője.

Az elmélet szerint a képzeletbeli szitán pedig áthullanak a „jók” és fennakadnak a „rosszak” vagy a gyanús elemek. Ugyanakkor a megfigyelőket is csak az tartja vissza attól, hogy visszaéljenek a munkájukból adódó lehetőségekkel, ha őket is állandóan megfigyelés alatt tartjuk, no és természetesen meg kell figyelnünk a megfigyelőket megfigyelőket is. Ez a leegyszerűsített gondolatmenet jól mutatja a kukkoló társadalom kialakulásának egyik fontos ideológiáját, amelyet akár még a hatékonysági mutatók is alátámaszthatnak. De egy ilyen társadalomkép, gondolom, ugyancsak messze esik az információs társadalommal kapcsolatos elveinktől és elképzeléseinktől.

Nem feledkezhetünk meg a fogyasztói attitűdökről és az azokat befolyásoló reklámpsziológia hatásairól sem. A „lebutított” felhasználó (akit máskor azért korholunk, hogy miért nem elővigyázatosabb és igényesebb) felületes és türelmetlen, könnyen befolyásolható, a kritikus gondolkodás képességét szinte elveszítette, mindenre rákattint, és ha valami nem töltődik két másodperc alatt a képernyőjére, azonnal megnyomja a stop gombot. Nagy kérdés, hogy ezek a beépített megfigyelést tartalmazó szolgáltatások vajon a felhasználók valós szükségleteit segítik-e ki-elégíteni, avagy egyszerűen a szolgáltatási túlkínálat eladásáról van szó; esetleg arról, hogy olyan fogyasztói és reklámpsziológó-

giai helyzetet teremtünk, amikor a felhasználót rászoktatjuk egy vonzó szolgáltatás használatára, és utána már nem tud megenni az arra épülő másik szolgáltatás használata nélkül.

Mit gondolnak a megfigyelők?

A kukkoló társadalom haszonélvezői között természetesen vannak cinikusok, akik arra hivatkoznak, hogy a cél (értsd: a profit vagy a hatalmi előny megszerzése) szentesíti az eszközt, vagy arra, hogy amúgy is az erősebb kutya dominál a falkában, vagy színleg elfogadják a jog és az etika szabályait, de a hátunk mögött összekacsintanak, vagy egyszerűen azt állítják, hogy „ez van, tessék tudomásul venni”. Ugyanakkor nem kevesen vannak, akik szeretnék a kialakult helyzetet magukban igazolni, legitimálni, egyértelműen pozitívnak tekinteni, és ehhez igazolásképpen illúziókat hívnak segítségül – olyan illúziókat, amelyek alapjai igencsak megkérdőjelezhetők.

A modernizmus vissza-visszatérő, klasszikus illúziója, hogy a technika megoldja a társadalmi problémákat. Ilyen illúzió az is, hogy a korszerű IKT és a megfigyelési technikák is megoldják a társadalmi problémákat, például a bűnözés problémáit. Igen, a technika megold bizonyos társadalmi problémákat, és azonnal újakat kreál. Vagyis jelentősen átalakítja az életviszonyokat, de valójában nem oldja meg, csak átstrukturálja a problémákat.

Egy másik, a műszaki értelmiség körében elterjedt illúzió (nevezhetjük téveszmének is) az, hogy „a technika semleges, jóra és rosszra is fel lehet használni”. Ezzel szemben világosan látható, hogy a technika mindig magán viseli kifejlesztőinek, pontosabban megrendelőinek ideológiáját, tükrözi érdekeiket, és ez így van a megfigyelés rendszereivel is.

Ugyancsak régi illúzió az, hogy az ideális társadalmat a mérnökök, vagy közelebbről az informatikusok és az informatikai rendszerek irányítják, ezt korábban „kibernetikus”, majd „összehuzalozott” társadalomnak nevezték, manapság digitális társada-

lomnak nevezik. Emögött az az elképzelés áll, hogy a társadalom nem önszerveződő, amelynek működését az állam mint erőszak-szervezet csak a lehető legszükségesebb mértékben korlátozza, hanem igazgató. Más szóval, nem önmagát megszervező, hanem felülről vezérelendő. Egy magyar államtitkár a közelmúltban egyenesen „informatikailag vezérelt” társadalomról beszélt.

Az illúziók mellett azonban konkrét érvekkel, érvelési rendszerekkel is találkozhatunk. Ezek a következők:

- Költségcsökkentés. Az adatvédelem rontja az üzletet, pénzbe kerül (ez igaz, de egy igényes felhasználói körnél még üzleti előny is lehet, ha tisztességesen bánunk az adataikkal).

- Versenyelőny. Többet kell tudnunk rólad, mint amennyit a versenytársaink tudnak (inkább legális és etikus pályán versenyezzenek a riválisok).

- Hatékonyság. A centralizált, az adatokat összekötő állam olcsóbb és hatékonyabb a decentralizáltnál (de tegyük hozzá: egy diktatúra is olcsóbb és hatékonyabb egy demokráciánál).

- Jóléti szolgáltatások, pozitív megkülönböztetés. Tudnunk kell, ki vagy, hogy segíthessünk rajtad (pedig enélkül is sokat lehetne segíteni).

- Antiterrorizmus. Aki nem jár a tilosban, „nincs félnivalója” (viszont: aki nem jár a tilosban, azt illegális és etikátlan megfigyelni).

- „Józan ész”. Hová jutnánk, ha minden szabályt betartanánk a kedves ügyfél érdekében? (Ha józan ész az üzleti vagy igazgatási érdeket értjük, akkor ez az érv csak az érdekeink retorikai legitimálását célozza.)

- Az ügyfeleink ezt akarják. Kényelmet és jobb kiszolgálást nyújtunk számukra (a valóságban nincs is valódi alternatívájuk).

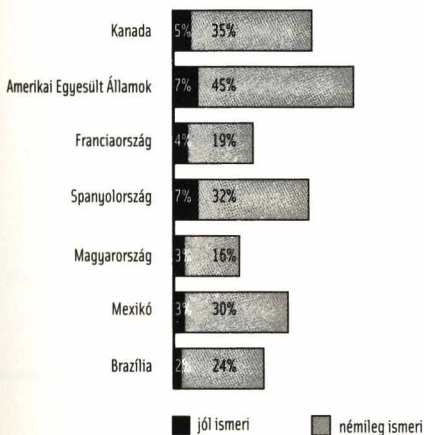
- Csak a gép gyűjti az adatokat, mi nem vagyunk rájuk kíváncsiak (mintha azt mondanánk: nem én voltam, csak a kezem).

És ha minden érv elfogyott, akkor jönnek az agresszívabb kérdések: Hogy képzeled, hogy ingyen kaphatsz internetet?! Vagy a legáltalánosabb, egyben hamis közhely: Miért, talán van valami titkolnivalód?!

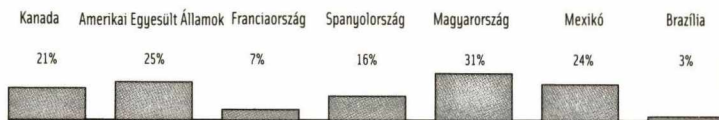
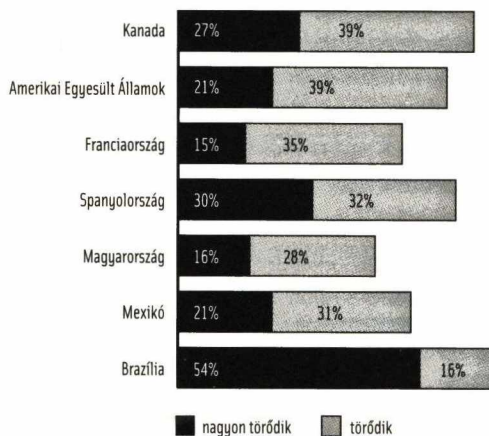
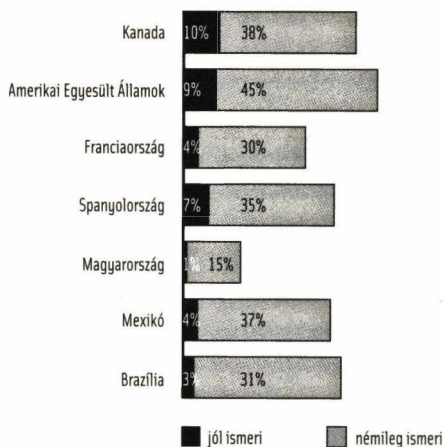
Mit gondolnak a megfigyelték?

Az utóbbi évek egyik legjelentősebb nemzetközi vizsgálata a lakosság megfigyeléssel és adatkezeléssel kapcsolatos véleményéről, amelyben Magyarország is szerepelt, a kanadai Queen's Egyetem által koordinált Global Protection of Data (GPD) kutatás. Kilenc, különböző gazdasági fejlettségű, kulturális hagyományú és politikai berendezkedésű ország: Brazília, az Egyesült Államok, Franciaország, Japán, Kanada, Kína, Magyarország, Mexikó és Spanyolország ezer-ezer lakosát, összesen 9606 embert kérdeztek meg egységes módszertannal. Az Ipsos véleménykutató cégcsoport nemzeti szervezeteinek közreműködésével többek között arról tájékoztak, hogy mennyire ismerik az elektronikus megfigyelés technológiáit, a magánszférát védő törvényeket, milyen – általuk érzékelt – megfigyelés alanyai voltak, és hogyan ítélik meg helyzetüket és beleszólási esélyeiket. A kérdőívet országonként két-két fókuszcsoportos interjú egészítette ki.

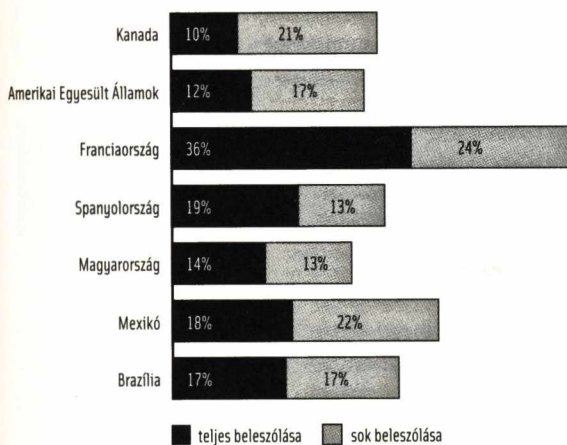
A jelentős kulturális különbségeket feltáró kutatás részletes elemzésétől itt el kell tekintenünk, de illusztrációként álljon itt néhány jellemző grafikon a magyar lakosság talán meglepő – és engedtesék meg: nem túl hízelgő – ismereteinek és attitűdjeinek érzékeltetésére.



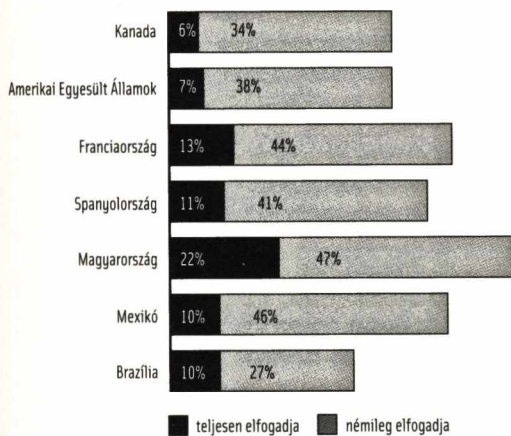
1. grafikon.
Ismeri
az adatvédelmi
törvényeket?
(magánszektor)



4. grafikon. Megesett Önnel, hogy a munkáltatója megfigyelte Önt?



5. grafikon.
Mennyi
beszéd van
adatai
sorsába?



6. grafikon.
Elfogadja
a fogyasztók
profilizását?

Ha összegezzük azokat kérdéseket, amelyek megválaszolásában Magyarország szélső értékeket mutatott, az alábbi eredményt kapjuk (4. táblázat).

A legmagasabb arányban...	A legalacsonyabb arányban...
...ér bennünket magánéleti sérelem a munkahelyen	...ismerjük az adatvédelmi törvényeket
...bízunk az állami és az üzleti adatkezelőkben	...érdekel bennünket adataink sorsa az interneten
...fogadjuk el, hogy a munkáltató átadja adatainkat a kormányzati szervezetnek	...tartjuk invazívnak a nemzetbiztonsági jogszabályokat magánéletünk szempontjából
...fogadjuk el a videokamerák alkalmazását	...gondoljuk, hogy van beleszólásunk adataink sorsába
...fogadjuk el a nemzeti személyazonosító kártyákat	...teszünk valamit adataink védelmére
...fogadjuk el a fogyasztói profilírozást	...lépünk fel a magánéletünkbe való behatolás ellen

4. táblázat. A magyarországi megkérdezettek válaszainak összefoglalása a szélső értékeket mutató kérdésekben

Ez a profil, amely a felmérés alapján látható, meglepő lehet, ha arra gondolunk, hogy Magyarországon 1992 óta van adatvédelmi törvény, és tizenöt éve működik adatvédelmi biztos, akinek tevékenysége nyomon követhető a médiában is. Ez megnyugtathatja a hivatásos megfigyelőket, vagyis a centralizációpárti köz-

igazgatás konzervatív informatikusait, a titkosszolgálatokat, az internetes üzleti világ képviselőit és a spamrobotok üzemeltetőit egyaránt, de nem nyugtathatja meg azokat, akik felelősséget éreznek az információs társadalom magyarországi kilátásai iránt.

És mit gondolnak az informatikusok?

Az eddigi vizsgálatok a „polgárookra”, a fogyasztókra, az internet-használókra, a diákokra és más populációkra irányultak, az informatikusok azonban valahogy kimaradtak a vizsgált csoportok közül. Márpedig ha a „kód” írja a törvényt, akkor az informatikusok ennek a világnak a tulajdonképpeni törvényhozói, szabályozói, akiknek az ismeretei, véleménye és attitűdjei meghatározó szerepet játszanak abban, hogy milyenek lesznek azok az informatikai rendszerek, amelyek kezelik adatainkat, elősegítik vagy korlátozzák a lakosság megfigyelését. Más megfogalmazásban: fontos szereplők, akik az etikai megfontolásokat technikai tudásukkal támogatják, vagy éppen más irányt segítenek elő. Az ő tudásuk kell az adatok védelméhez vagy éppen megszerzéséhez is. Véleményük megismerésének hiányát egy jelenlegi, holland és magyar szervezetek részvételével zajló európai uniós projekt, a BROAD¹⁸ kívánja pótolni, amelynek magyar online kérdőívvel esetleg az olvasó is találkozhatott.

Az online kérdőív mellett mindkét országban személyes interjúk is készültek, ehelyütt ezek tanulságaiból ismertetünk néhányat. A vizsgálat két, eltérő kulturális környezetet képviselő országban, de egy globalizálódó szakmában készült. Ennek megfelelően találkozhatunk országtól függő eltérő jellegzetességekkel és közös véleményekkel egyaránt. Az alanyokat úgy választották ki, hogy az informatikai szakma különféle ágazatait, a tevékenységek és munkahelyi szerepek széles skáláját képviseljék.

Az interjúk egyik témaköre az internetes kommunikáció és a megfigyelés kockázataira vonatkozott az adatalanyok szempontjából. Itt jelentős volt az eltérés a két ország informatikusai-

nak megítélése között: a holland interjúalanyok aggasztónak tartották a helyzetet, míg a magyarok többsége úgy vélte, „ez van, ez a mai valóság”. Az informatikusok felelőssége tekintetében is eltérést találunk: a holland interjúalanyok esetében jóval több etikai megfontolással találkozhatunk, míg a magyarok többsége úgy véli: „ez nem az én dolgom.”

Hasonló volt azonban a két ország informatikusainak véleménye a munkahelyi megfigyelésekkel kapcsolatban. Általában a dolgozókkal és nem a megfigyelőkkel szolidárisak, bár nem utasítják el a megfigyelés minden formáját. Az állam általi megfigyeléssel szemben mindkét ország informatikusai jóval toleránsabbak, és úgy vélik, hogy az állam egyik fő feladata a biztonság garantálása.

A holland interjúk elemzéséből kiderül továbbá, hogy az informatikusok

- úgy érzik, hogy van befolyásuk;
- azt látják, hogy a döntések többsége csoportos döntés (amit általában támogatnak);
- azt gondolják, hogy a magánélet védelme egyenlő az adatbiztonsággal;
- úgy érzik, hogy tudatosabbak, mint az átlagos polgár;
- kifejezik véleményüket, hogy ezekkel a kérdésekkel többet kellene foglalkozni nyilvános fórumokon;
- nem ismerik a PET-eket (Privacy Enhancing Technologies),¹⁹ és nem is mutatnak érdeklődést irántuk;
- nem érzik magukat felelősnek az adatvédelmi törvények betartásáért;
- úgy gondolják, hogy a felelősség a felső vezetésé;
- úgy érzik, hogy a jogászok mindig későn szólnak bele és akadályozzák a munkát;
- ugyanakkor nem számoltak be a jogszabályok szándékos megkerüléséről.

További vizsgálatok tárgyát képezi, hogy ezek a nézetek hogyan tükröződnek a tervezett és megvalósított adatkezelő rendszerekben, és mennyire közvetlenül befolyásolják a megfigyelő-

rendszerek infrastruktúráját és működését. A BROAD-kutatás célja azonban nemcsak az, hogy feltérképezze az informatikusok véleményét a személyes adatok kezeléséről, és hogy más országokban is megismételhető módszertant dolgozzon ki erre, hanem az is, hogy az eredményeket visszacsatolja az informatikus társadalom fórumaiba, az oktatásba, a szakmai szervezetek munkájába, az online fórumokba, nemzetközi konferenciák programjába – egyszerűen hogy szembesítse az informatikusokat saját véleményükkel: tényleg ilyenek vagyunk?

Válaszok a kihívásra

A tudomány legfontosabb válasza a kukkoló társadalom kialakulására az, hogy megindult az egész jelenség multidiszciplináris vizsgálata, sőt új diszciplína jött létre, a Surveillance Studies, amit talán megfigyeléstannak fordíthatnánk. Ez a tudományág azonban nem azzal foglalkozik – mint először sok érdeklődő megfigyelő gondolja –, hogy hogyan lehetne növelni a megfigyelés hatékonyságát, hanem a megfigyelés és a megfigyeltség társadalmi hatásait kutatja. Kiváló kutatóhelyek jöttek létre, mint például az észak Harvardjának is nevezett Queen's Egyetemen (Kingston, Kanada) a Surveillance Studies Centre, a londoni City University pedig már mesterképzést is hirdet megfigyeléstanból. Tudományos igényű folyóiratok jöttek létre a témában, például a *Surveillance & Society*, és tudományos igényű kutatási projektek indultak, mint például az UrbanEye, a Living in a Surveillance Society (LiSS), vagy a fentebb említett Global Protection of Data (GPD).

A technológiának is van válasza: az elmúlt évtizedekben létrejöttek a privátszférát erősítő technológiák, a PET-ek, amelyek megkísérlik megakadályozni a személyes adatok szükségtelen vagy jogellenes felhasználását, vagy olyan eszközöket és beavatkozási lehetőségeket kínálnak, amelyek növelik az egyén ellenőrzését személyes adatai felett – és mindezt anélkül, hogy csökkentsék az információs rendszer funkcionalitását. A PET-ek el-

ső generációja egy-egy probléma megoldására született: így jöttek létre az anonim böngészők, a webpoloskairtók, a nym-generátorok, a profilgátlók, az anonim remailerek, az adatvédelmi bizalmi védjegyek, a cookie-irtók, az anonim digitális pénzrendszerek, a spyware-irtók, a bioscrypt, és sok más technológia és alkalmazás; még a megfigyelés egyik legagresszívebb technikái megoldásának tartott RFID-technológiának is van PET-változata.²⁰ A PET-ek új generációja rendszerszemléletű, a teljes információs hálózatot kívánja átfogni, mint a PRIME, amely nem a megfigyelő, hanem a megfigyelt fél számára nyújt felhasználócentrikus identitásmenedzsmentet és szerep alapú magánszféravédelmet.

A valós életben ugyanis más-más információt osztunk meg a családukkal, a barátainkkal, az üzleti partnereinkkel; a közértben nem kéri a személyi igazolványunkat, a kórházban a diplománkat – és természetesen nem azért, mert valami „titkolnivalónk” lenne, hanem azért, mert nem tartozik rájuk. Ez a társadalmi szerep alapú információs rendszer bomlik meg az internetes megfigyelőrendszerek működésével, amelyek minden részinformációt igyekeznek összekötni és felhasználni. A PRIME ezt a természetes információs helyzetet próbálja visszaállítani a digitális világban is.

Noha a felmérések azt mutatják, hogy a PET-ek használata jelentősen nőtt az elmúlt években,²¹ látható, hogy sem a technológia, sem az ellentechnológia nem képes önmagában megoldani az univerzális megfigyeltségből adódó problémákat. Ezt felismerve a civil mozgalmaknak is kialakult a maguk válasza a problémára: tudatosító kampányokat folytatnak a lakosság körében, lobbiznak a politikusoknál, akciókat szerveznek, eltitkolt megfigyelési ügyek nyilvánosságra hozásával botrányokat szerveznek és jelentős sajtóvisszhangot keltenek.²² Az egyik legérdekesebb – és véleményünk szerint téves – elképzelés a „visszafigyelés”, a megfigyelők civil megfigyelése, aminek angol-francia szójátékkal a *sousveillance* nevet adták,²³ és aminek eredményeképpen létrejöhetne a felek közötti megfigyelési egyensúly, az *equivoillance*.²⁴

A civil válasz érdekes területe a kreatív alkotások létrehozása: filmek, videoklipek, grafikák, digitális montázsok, animációk és egyéb műfajú alkotások jöttek létre, amelyek témája a társadalom és az egyén megfigyeltsége. Vannak olyan alkotók, aki magukat *surveillance artist*-nak tartják, vagyis olyan művésznek, akinek központi témája a kukkoló társadalom és az egyén megfigyeltsége.²⁵ A BROAD-projekt keretében is létrejöttek magyar nyelvű, igen szórakoztató, ugyanakkor nagyon is komoly és színvonalas egyperces rövidfilmek,²⁶ amelyek az internetes megfigyeltségre hívják fel a néző figyelmét.

Mindezek a válaszok azonban nem elegendők arra, hogy megfordítsák az uralkodó trendet, és érdemben korlátozzák a kukkoló társadalom gyakorlatát.

Tanulságok – avagy hogyan éljünk egy kukkoló társadalomban?

A folyamatos megfigyelés társadalma eljött, ebben éljük mindennapjainkat. Azt nem tehetjük meg, de nincs is rá szükség, hogy digitális absztinenciát hirdessünk, és ne használjunk mobilt, internetet, bankkártyát, ne váltsuk ki gyógyszereinket, vagy bezárkózzunk, és ne élvezzük az új technológiák előnyeit. Üldözési mániát sem szabad kialakítanunk magunkban csak azért, mert mindig követnek, megfigyelnek. De egy olyan társadalomban, ahol a szabad akarat, az egyén autonómiája még számít, ahol az állam beavatkozása a magánéletbe és az üzleti monopóliumok befolyása korlátozott, ott fontos ébren tartani vagy újból felbresszteni az igényt magánéletünk és mások magánéletének tiszteltetésében tartására.

De van-e még függöny virtuális ablakunkon? Talán még van, bár egyre vékonyabb, és sajnos nem tartozik virtuális lakásunk alapfelszereltségéhez. Meg kell tervezni, meg kell „varratni”, néha még fizetni is kell érte, de legfőképpen be kell húzni, ha nem egy képzeletbeli üvegfalú házban vagy az Elvarázsolt Kastély tükörmében²⁷ kívánjuk élni mindennapjainkat.

Egy olyan generáció, amely információs magánélet nélkül nő fel, amelynek tagjai számára nem adatik meg a rendelkezés digitális énjük felett, nehezen érti meg ennek jelentőségét. Számukra nem a tiltás, a veszélyek emlegetése a fontos, hanem a pozitív példák, a magánélet és az önrendelkezés mint érték megjelenítése. A legfontosabb azonban annak felismerése, hogy a technika ma már mindent lehetővé tesz, de nem szabad hogy a technika és a mögöttük állók irányítsák az életünket. Ismét meg kell tanulnunk, hogy nem mindent szabad, amit lehet, és nem mindent illik, amit szabad.²⁸

Demetrovics Zsolt

Pszichológus, kulturális antropológus (Eötvös Loránd Tudományegyetem Addiktológiai Tanszéki Szakcsoport)

Koronczai Beatrix

Pszichológus (Eötvös Loránd Tudományegyetem Addiktológiai Tanszéki Szakcsoport)

AZ INTERNETFÜGGŐSÉG NÉHÁNY PSZICHOLÓGIAI VONATKOZÁSA

Az internet megjelenését követően igen hamar világossá vált, hogy annak hatalmas előnyei mellett problémákkal is számolnunk kell ezen új médium vonatkozásában. Kimberley Young¹ 1998-ban megjelent kötete mutatta be elsőként az internetfüggőség (internetaddikció) jelenségét számos esettel, interjúval illusztrálva a problémát. A félig ismeretterjesztő, félig tudományos mű hatalmas érdeklődést keltett. A Young által spontán módon összeállított húsztételes kérdőív mindenféle pszichometria ellenőrzés nélkül hatalmas karriert futott be, s maga az internetfüggőség koncepciója is sikeresen vert gyökeret a pszichológiában, pszichiátriában. Bár a jelenség önálló betegségként történő értelmezését az elmúlt évtizedben folya-

matos vita övezte, az Amerikai Pszichiátriai Társaság (APA, American Psychiatric Association) mentális zavarokat osztályozó rendszerének jelenlegi átdolgozása során az internetaddikció már a kapukat döngeti. Az APA által 2013-ban kiadásra kerülő Diagnosztikus és Statisztikai Kézikönyv 5. (DSM-V) verziója ugyan önálló zavarként még nem fogja tartalmazni az internetaddikciót, de a függelékben már szerepelni fog ez az amúgy igen rövid történetre visszatekintő zavar, ami az alig egy évtizedes múltat figyelembe véve igazi „sikertörténetnek” tekinthető. Mi több, a témának ma már önálló szaklapja is van *Cyberpsychology and Behavior* címen.

Az internetfüggőség jelensége

De mi is valójában az internetfüggőség, az a jelenség, amelynek sem a létezéséről, sem a nevééről nincs teljes egyetértés a pszichológiai, pszichiátriai szakmán belül? A betegség elnevezésére többféle terminológia merült fel az évek során. Az internetaddikció vagy internetfüggőség mellett felmerült a patológiás, a túlzott (excesszív), a maladaptív,² a problémás vagy a kompulzív internethasználat elnevezés. Az elnevezések közül a legelterjedtebb talán az internetfüggőség és a problémás internethasználat, az utóbbi kettő elkülönítése azonban az egyik kulcsfontosságú kérdés, legalábbis a klinikai vonatkozásokat tekintve.

Az internetaddikció elnevezés ugyanis egyértelműen betegségre utal, azaz feltételezi, hogy a jelenségnek létezik egy patológiásnak tekinthető, más mentális és viselkedészavaroktól – kóroktanilag, diagnosztikai és terápiás jellemzőit tekintve – jól elkülönülő formája, amit függőségként azonosíthatunk. A megfogalmazás ezt nem zárja ki, de nem is állítja, pusztán azt jelzi, hogy létezik az internethasználatnak egy problémás, az alkalmazkodást rontó formája. Ez a megközelítés azonban nem foglal egyértelműen állást a tekintetben, hogy az internetfüggőségként azonosított tünetek együttesét érdemes-e külön betegségnek tekinteni, vagy egyszerűen egyéb zavarokat (pl. szorongást, depressziót) fedő tünetekről,

tünetcsoportról van szó. Utóbbi felvetés tehát nem zárna ki azt sem, hogy nem önálló betegséggel állunk szemben, hanem a problémás internethasználat tünetei egyszerűen egyfajta választ jelentenek egyes emberek problémáira.

Nincs teljes konszenzus abban sem, hogy milyen kritériumrendszer alapján határozzuk meg és mérjük az internetfüggőséget. Scott Caplan amerikai szakember elsődlegesen a jelenség kognitív és viselkedési jegyeit hangsúlyozza és tartja meghatározónak, és a későbbi kutatások egy része szintén ezen a csapáson halad. Dominánsabb azonban az internetfüggőséget az addiktológiai zavarokkal, illetve az impulzuskontroll-zavarokkal³ rokonító megközelítés. Bár a kezdeti meghatározások ezen utóbbi két csoport mentén is hasadtak, így egyesek inkább az impulzuskontroll zavaraival, elsősorban a kóros játékszenvedéllyel, míg mások inkább a pszichoaktív szerekkel kapcsolatos függőséggel rokonították az internetfüggőséget, ez az elkülönítés egyre inkább értelmét veszti. A már említett DSM-V például már maga is egy csoportban fogja tárgyalni a szerencsejátékkal és az alkohollal vagy egyéb drogokkal kapcsolatos függőségeket, felismerve, hogy ezek háttérben nagyon hasonló mechanizmusok állnak.

Mint említettük, Kimberly Young volt az első, aki a túlzott és problémát jelentő internethasználatot addiktív zavarként írta le. Rámutatott, hogy a problémás használók elveszítik a kontrollt internethasználatuk felett, fokozottan belemerülnek az internetezésbe, képtelenné válnak arra, hogy csökkentsék internetezésüket annak ellenére, hogy az számukra problémát okoz. Young, bár az internetfüggőségről mint addiktív problémáról beszél, az általa kidolgozott szempontrendszerben mégis inkább a kóros játékszenvedély kritériumaira alapozott. Young szerint az tekinthető internetfüggőnek, akinél az általa leírt nyolc tünetből legalább öt észlelhető. A Young által számba vett tünetek a következők:

- Az internettel való intenzív foglalkozás (a korábbi online aktivitásra gondolás vagy a jövőbeli anticipálása).
- Ugyanakkora öröm eléréséhez megnövekedett idejű online jelenlét (tolerancia).

- Ismételt erőfeszítés az internethasználat csökkentésére vagy abbahagyására.
- Idegesség, depresszió vagy hangulati labilitás, amikor az internethasználatot korlátozzák.
- Az előre eltervezettnél hosszabb online időtöltés.
- Az internethasználat miatti munkavégzésbeli vagy kapcsolati károsodás.
- Hazudozás másoknak arról, hogy mennyi időt tölt internethasználattal.
- Internethasználat hangulatszabályozás céljából.

Mások kritizálják Young rendszerét, az igazi problémát azonban az jelenti, hogy egyik megközelítés sem alkalmaz olyan klinikai vizsgálatot, amelynek alapján valóban meg lehetne határozni azt a pontot, ahol elkülönül a problémás internethasználat és az internetfüggőség.

Griffiths 1998-as publikációjában az internetfüggőséget technológiai addikcióként határozza meg, és a viselkedési addikciók közé sorolva hat kritérium mentén definiálja. Az internetfüggőség viselkedési addikcióként történő meghatározásakor az internethasználat maladaptív mintázata képezi a definíció alapját. Eszerint a személy ismétlődő, tolakodó sürgetést érez arra, hogy véghezvigye azt a cselekvést (az internetezést), amely aktuálisan örömet szerez számára, de a későbbiekben distresszhez és/vagy a mindennapi funkciók károsodásához vezet. A hat tünet Griffiths szerint a következő:

- A kiemelkedőség (szaliencia) arra utal, hogy az internetezés az egyén életének legfontosabb részévé válik, dominálja gondolatait, érzelmeit és viselkedését, azaz kiemelkedik az egyéb viselkedések közül. Az internet tehát *uralja* a személy mindennapjait; gondolatait csakúgy, mint érzéseit (sóvárgás) és viselkedését. Amikor nem internetezik, gondolatai gyakran akkor is az internet körül forognak.

- A tolerancia az addiktív zavarok egyik kulcstünete, ami arra utal, hogy egyre nagyobb mennyiségű internetezésre van szüksége a személynek az elvonási tünetek elkerüléséhez, illetve annak érdeké-

ben, hogy megfelelően érezze magát. A tolerancia tehát az internetezés gyakoriságának és hosszának (idejének) növekedését jelenti.

– Bár a megvonási tünetek megjelenését elsődlegesen a drogokhoz kötjük, valójában ezek a viselkedési addikcióknak is karakterisztikus jellemzői. Az internetfüggő esetében is kialakulhat tehát jellegzetes megvonásos tünetegyüttes, amely kellemetlen testi-lelki állapotot takarhat. A leggyakrabban jelentkező tünetek: idegesség, irritabilitás, szorongás, hangulatingadozás, rosszkedv stb.

– Kulcsfontosságú tünet a konfliktusok megjelenése. Ez a tünet az internetezés okozta konfliktusokra utal; jelentkezzenek akár az érintett egyén és környezete között (szociális konfliktus), akár az élet egyéb területein (munka, szociális kapcsolatok, érdeklődés), esetleg saját magával szemben (személyes konfliktus).

– Szintén fontos és jellegzetes tünet a hangulatmódosítás. Ez a tünet arra a szubjektív élményre utal, amelyet az egyén az internetezés következményeképpen tapasztal. Ilyen lehet a „feldobottság”, az eufória érzete, vagy a másik oldalról a negatív hangulati állapotok (szorongás, depresszió) megszűnése.

– Végül fontos tünet a visszaesés (relapszus) tünete is. Ez a korábban megszokott, rendszeresen művelt cselekvéshez, azaz az internetezéshez történő újbóli visszatérésre utal egy-egy kihagyott időszak után. Ez a kiesés adódhat az egyéntől függő, de akár az egyéntől független okból is; a lényeg, hogy a személy nem képes tartósan korlátozni vagy visszafogni internetezésének mértékét.

Az utolsó jelenség megítélése ugyanakkor árnyalt szemléletet igényel, hiszen sok más addikcióval (elsősorban a pszichoaktív szerekkel kapcsolatos függőségekre gondolhatunk itt) szemben jelen esetben nem cél a teljes absztinencia.

Általános és specifikus jelenségek az internetfüggőségben

Bár kezdetben csak általában internetfüggőségről esett szó az irodalomban, hamar világossá vált, hogy nem magától értetődő, hogy egységes jelenségről lenne szó. Davis 2001-ben ezzel össz-

hangban specifikus (egy bizonyos funkció, pl. online játék, chat vagy pornográfia az internethasználat célja) és generalizált (az internet multidimenzionális túlhasználata) internetfüggőségről beszél. Young, Pistner, O'Mara és Buchanan 1999-ben korai felosztásukban az internetfüggőség öt típusát írták le – ezek:

- kibersexuális addikció;
- kiberkapcsolati addikció;
- netkompulzió (pl. szerencsejáték vagy internetes vásárlás);
- túlzott információszerzés (kompulzív böngészés);
- számítógép-addikció (túlzott játék).

E felosztás azonban ma már mindenképp meghaladottnak tekinthető.

E felosztással szemben elfogadottabb az a nézet, hogy egy online szerencsejátékos elsődlegesen szerencsejátékos, és esetében az internet, illetve funkciói csak közvetítői, eszközei, megjelenési felületei a problémának. Hasonlóképp az online játékoktól függő személy vagy a kompulzív online pornográfiafogyasztó esetében is alapvetően onlinejáték-függőségről, illetve szexuális addikcióról beszélhetünk, s nem internetfüggőségről.

Az internetfüggőség elterjedtsége

Az internetfüggőség elterjedtségére, prevalenciájára vonatkozóan nagyon eltérő adatok állnak rendelkezésre. Nehezíti a becslést, hogy nincs konszenzus sem a tünetekben, sem a mérőeszközben; egyelőre tehát nem áll rendelkezésünkre olyan kritériumrendszer, amely egységesen alkalmazható lenne, így a különböző kutatók eltérően húzzák meg a határt a probléma mérésénél.

Aboujaoude, Koran, Gamel, Large és Serpe 2006-ban megjelent tanulmányukban a teljes felnőtt lakosság körében az Egyesült Államokban 0,3–0,7% közötti értéket valószínűsített, de egyetemisták vagy középiskolások körében általában magasabb értékek mutatkoznak. Norvég serdülők (átlagosan 15 évesek) reprezentatív mintáján például Johansson és Götestam 2004-ben 2%-os

értéket mért. Egy hazai vizsgálat során a szerző és munkatársai internetezők nem reprezentatív (1037 fő, 54,1% férfi; átlagéletkor 23,3 év; 9 és 69 év közöttiek) mintáján 4,3%-ra becsülte a problémás internethasználók arányát. Távol-keleti vizsgálatok általában az európai és amerikai eredményekhez képest magasabb prevalencia-értékeket találnak. A klinikai vizsgálatok és a diagnosztikus konszenzus hiánya miatt ugyanakkor mindezen vizsgálatok eredményei csak nagyon korlátozottan értelmezhetők.

Az internetfüggőség hátterében rejlő problémák

Az internet megjelenését követően az internetfüggőség definícióját elsődlegesen az internethasználat időtartamához kötötték: eszerint a heti 38 órát meghaladó használat számított problémásnak. Ez a nyilvánvalóan leegyszerűsítő és félrevezető megközelítés aztán sokat finomult. Nyilvánvalóvá vált, hogy vannak olyan internethasználók, akik intenzíven használják ugyan az internetet, mégsem mutatják az internetfüggőség jeleit. Egyértelművé vált, hogy az internethasználat kontextusa alapvető meghatározója a problémás használatnak; így a munkavégzésre használt internetezés időtartama nincs összefüggésben az internetfüggőséggel, míg a munkavégzésen kívüli internetezés időtartama igen, véli a szerző is.

Az internet számos alkalmazást kínál, amelyek nagyon különböző igényeket szolgálhatnak, s amelyek nagyon eltérő mértékben asszociálhatók a függőség jelenségével. A kutatások azt jelzik, hogy az internet legaddiktívabb területe egyértelműen az internet szociális aspektusa, azaz azok az alkalmazások, ahol a felhasználók más személyekkel tudnak kapcsolatba lépni az interneten keresztül. Ezen alkalmazások közül is elsősorban a szinkron (azonos idejű) interaktív alkalmazások tűnnek kockázatosnak a túlzott használat tekintetében. Ennek során a felek azonos időben vannak jelen és lépnek interakcióba egymással (pl. chat, online játék, azonnali üzenetek váltása). Ezen alkalmazásoknál nem kell hosszú ideig várni a válaszra, az azonnali-

ság maradéktalanul teljesül, márpedig ez az azonnaliság, azaz a késleltetés képességének hiánya minden addiktív magatartás kulcstünete. Könnyű ugyanis belátni, hogy az addikció tekintetében elsődlegesen az olyan alkalmazások kockázatosak, ahol az adott cselekvés és következménye közötti kapcsolat közvetlen és azonnali.

E tekintetben például az e-mail használata, ahol a válasz késleltetett, sokkal kevésbé valószínű, hogy intenzifikálódik, mint a chathasználat, ahol a reakció azonnali. Hasonló a helyzet más addikcióknál is: a késleltetettség az oka például, hogy a lottó, amelynek eredményére napokig kell várnunk, sokkal kevésbé vezethet függőséghez, mint a nyerőautomaták, ahol az eredmény azonnali.

A kommunikáció történhet olyan emberekkel, akiket a személy nem az interneten ismert meg, vagy akikkel az interneten kívül is találkozik, illetve használhatják az internetet új kapcsolatok kiépítésére, és az azon való kapcsolattartásra is anélkül, hogy a kapcsolat átfordulna személyes találkozásba. Több külföldi és hazai kutatás jelzi, hogy a problémás használat elsősorban az új kapcsolatok létrehozása céljából történő internetes kommunikációval függ össze. A kutatások arra is felhívják ugyanakkor a figyelmet, hogy a családdal, barátokkal történő online kommunikáció, legyen az akármilyen intenzív, nem eredményez problémás internethasználatot.

Ez a jelenség is jól mutatja az internet használatának kettős jellegét, amelyben annak előnyeit és kockázatait nagyon nehéz különválasztani. Az internet szerepe alapvető lehet a szociális támogatásban, a depresszió, a magány enyhítésében, egyáltalán a kapcsolatteremtésben, ami mai elszigetelt, individualizálódott társadalmunkban igen fontos funkció. Ugyanakkor amellet, hogy az internet csökkentheti ezt az elszigeteltséget, egyidejűleg alapvető kockázatot is jelent annak elmélyítésében. Csepeli György 1997. évi jellemzése szerint az online kommunikáció olyan helyzet, amely sem nem magány, sem nem társaság. Másfelől nézve azonban egyszerre lehetőség a magány elűzésére és a kapcsolódásra, de magában rejt az izoláció veszélyét is.

Az internet kommunikációs jellegzetességei

A problémás internethasználat okainak feltérképezése során magának az internetnek mint médiumnak a jellemzőit is vizsgálnunk kell. A legfontosabb és legszélesebb körben tárgyalt ilyen jellegzetesség az anonimitás. Az anonimitás csökkenti a másokkal való interakció keltette szorongást. Anonim helyzetben az emberek közvetlenebbek, nyitottabbak, aminek következtében a kapcsolatok gyorsabban érik el az intimitás mélyebb szintjét, a közelség érzését. Csökkenti továbbá a társas interakciótól való szorongást az is, hogy az internethasználó jobban tudja kontrollálni az interakciót. Bármikor kiléphet belőle, illetve az online kommunikáció tempója könnyebben szabályozható, mint a szemtől szembeni kommunikáció ritmusa. Az énbemutatás és benyomásformálás kontrollját is kiemeli az észlelt előnyök kapcsán, amelyek ismételtén hozzájárulnak az interakciók gyors elmélyüléséhez. Az internet interaktív lehetőségei a valóságos, fizikai egyedüllét ellenére a másokkal való kapcsolatban állás érzését keltik. A fizikai jelenlét hiánya következtében pedig a nem, az életkor, az etnikai hovatartozás, a szocioökonómiai státus, a földrajzi elhelyezkedés, a családi állapot, a valós vagy vélt testi fogyatékoságok rejtve maradnak a partner számára, és lehetővé válik a szabad önkifejezés, vagy akár egy új, csak online létező személyiség, identitás kifejlesztése. Az internet könnyű hozzáférhetősége, elterjedtsége és olcsósága is mind-mind olyan tényezők, amelyek lehetővé teszik annak kiterjedt használatát.

Internetfüggőség, személyiség és pszichológiai tünetek

Az internetfüggőség szoros kapcsolatot mutat a *depresszióval*, állítja több külföldi és hazai kutató. Nehéz ugyanakkor az ok-okozati kapcsolat megállapítása, így egyaránt elképzelhető, hogy a fokozott internethasználat következményeként jelennek meg hangulati problémák, illetve, hogy a depresszív tünetek nyomán fordul va-

laki az internet felé, amely segít kompenzálni tüneteit, elterelni gondolatait a problémáiról, vagy enyhíti depresszióját az interneten elérhető szociális támasz, pozitív élmények, kapcsolatok által. A leginkább valószínű azonban, hogy a két folyamat kölcsönösen hat egymásra, azaz a kezdeti hangulati problémák hozzájárulhatnak a fokozott internethasználathoz, amely azonban hosszú távon – ha nem is minden esetben – ronthatja a tüneteket.

A kutatások alapján azok az internethasználók, akik hajlamosabbak a magányosabb, szociálisan inaktív életstílusra, nagyobb eséllyel válnak problémás internethasználókká, mint szociálisan aktív társaik. Szintén egyértelmű összefüggés mutatkozik a problémás internethasználat és az alacsony önértékelés között. Mind a magányosság, mind az önértékelés esetében – hasonlóan a depresszióhoz – kölcsönös ok-okozati viszony feltételezése a legvalószínűbb.

Született néhány longitudinális vizsgálat is az ok-okozati viszonyok kiderítése céljából. Kraut és munkatársai 1998-ban korai vizsgálatukban 169 fő esetében követték nyomon az internethasználat hatását a családi kommunikációra, a pszichológiai jólétre és egyéb szociális kapcsolatokra az internet bekötésétől kezdve az első egy-két éven át. Eredményeik azt mutatták, hogy a nagyobb mértékű internethasználat a családi kommunikáció és a szociális kapcsolatok csökkenésével, továbbá a depresszió és a magányosság növekedésével kapcsolódott össze.

Megfogalmazták az internet paradoxonjának tételét, miszerint bár az emberek az internetet elsősorban kommunikációra használják, a fokozott használat inkább a szociális bevonódottság és a pszichológiai jóllét csökkenésével járt együtt. Magyarázatként felmerül, hogy az emberek erős, valós kapcsolati kötődéseiket helyettesítik szegényesebb minőségű, új internetes társas viszonyakkal, amelyeket nem tudnak beágyazni korábbi kapcsolatrendszerükbe. Fontos eredmény azonban, hogy az internethasználat e negatív hatásai a vizsgálat harmadik évének végére eltűntek, azaz a kedvezőtlen következmények átmenetinek bizonyultak.

Bessiere és munkatársai 2008-as tanulmányukban az internetes kommunikáció újabb aspektusát vették górcső alá. Hat hó-

napos longitudinális vizsgálatuk eredményei szerint az internet-használat önmagában csak nagyon kis mértékben kapcsolódott a használók jóllétéhez. Ugyanakkor azok az emberek, akik a barátaikkal, családtagjaikkal való kommunikációra használták az internetet, csökkenő depressziót mutattak. Azoknál viszont, akik új emberekkel ismerkedtek meg az interneten, az internethasználat a depresszió növekedésével járt együtt. Ez a növekedés különösen azoknál volt szembetűnő, akiknek nagyobb volt a kezdő szociális támogatási szintjük, esetükben ugyanis valószínűleg a korábbi jelentős társas háló csökkenése, tulajdonképpen egyfajta magányosodás következett be. Akik kisebb szociális hálóval rendelkeztek és introvertáltabbak voltak, nem tapasztalták ugyanazt a depressziószint-növekedést.

Kezelés

Az internetfüggőség és a kóros szerencsejáték definíciós hasonlósága miatt ésszerű feltételezés, hogy az utóbbi zavar szokásos farmakoterápiás kezelése az internetfüggőség esetében is hatásos lehet. Az elsődlegesen felmerülő gyógyszerek ily módon az antidepresszívumok, illetve az opiát antagonistá naltrexon.⁴ Érdemi kutatás azonban e téren – részben az internetfüggő páciensek alacsony száma miatt – nem történt. Fontos ugyanis látnunk, hogy a fent jelzett prevalencia-adatok mellett sokan egyáltalán nem vagy nem közvetlenül az internetfüggőség miatt keresnek kezelést, hanem valamilyen társuló probléma miatt. A farmakoterápiának mindazonáltal épp emiatt fontos szerepe lehet a társuló zavarok, elsősorban a szorongásos és depressziós tünetek vagy az alvászavar kezelésében.

Young, aki elsőként írt az internetfüggőség pszichoterápiás kezeléséről, elsősorban viselkedésterápiás stratégiákat ajánlott. Elképzelése szerint a felmerülő viselkedésterápiás stratégiák a következők lehetnek:

- Az ellentét gyakorlása: azonosítani kell a személy internet-használati mintázatát, azután az online rutint próbálni megtörni

egy semleges aktivitással. Például ha a rutin szerint a személy az egész hétvégét online töltene el, akkor helyette töltsen a szombat délutánt házon kívüli aktivitással.

- Külsődleges fékek: a személy emlékeztetőket használhat (mint az óracsörgés), amelyek figyelmeztetik őt arra, mennyi időt tölt online.

- Célok felállítása: a nagyfokú motiváció és támogatás dacára az internetfüggők megszakíthatják a kezelést, ha nincsenek kitűzve világos célok. A napi vagy heti terv használata segítség lehet, amelyben meghatározott időkeretekhez köti az internethasználatot. – Emlékeztető kártyák: a személyt bátorítani kell arra, hogy írja le kártyákra az internethasználat negatív következményeit és a kontrollált online idő lehetséges előnyeit (pl. képes lesz több időt eltölteni a partnerével).

- Személyes leltár: internetfüggőként gyakran jelentős mennyiségű időt töltenek online, aminek következtében elhanyagolják más hobbijukat és érdeklődésüket. A személyt bátorítani kell arra, hogy listát csináljon korábbi aktivitásairól, ezáltal újraéledhetnek korábbi érdeklődései más tevékenységek iránt, amelyek nem kapcsolódnak az internethez.

Fontos azonban látnunk, hogy az internetfüggőségénél (akár csak pl. az évszavaroknál vagy a munkafüggőségénél) a gyógyulás céljaként semmiképpen sem a teljes absztinenciát, hanem a normalizált használatot érdemes kitűzni, hiszen az internetnek számos hasznos pozitív alkalmazása van, és szinte lehetetlen kizárni mindennapi életünkéből. Amennyiben azonban a függőség csak bizonyos alkalmazásokra (pl. online játékokra) vonatkozik, akkor ezekre vonatkozóan reális cél lehet a teljes absztinencia elérése is.

Z. Karvalics László *Történész, az információs
társadalom kutatója, a Szegedi Tudományegyetem
tanszékvezetője*

AZ UNIVERZÁLIS KVANTOR RÉMURALMA – AVAGY A VESZÉLYDISKURZUSOK LOGIKAI SZERKEZETÉRŐL

„Nos, én sosem olvasom az internetes sajtót, mert szerintem a netezők társadalomképtelen, sunyi alakok, akik nem merik nyíltan felvállalni a saját véleményüket, hanem jobban esik nekik arctalanul mocskolódni. Miért kellene, hogy érdekeljen, hogy Micu és Józsi megvitatják egymás között, hogy a Dévényi egy f--? Miért kellene, hogy érdekeljen?”

Minden magyar lemezlovas élő legendája, Dévényi Tibor („Tibi bácsi”) feltehetően olyasmit szeretett volna szenvedélyesen kifejezni idézett nyilatkozatában, hogy azok, akik őt anonim módon ócsárolják a neten, nem érdemesek arra, hogy ő mint érintett el is olvassa a véleményüket. Ha ezt nyilatkozta volna, nem kellene bevezetesképpen az ő soraival illusztrálni, hogy mekkora kárt okoz a gondolatok megjelenítéséhez óvatlanul választott nyelvi-logikai szerkezet. Különösen akkor gond ez, ha olyan

tárgyköréről van szó, amely amúgy is félelmekkel, előítéletekkel, felszínességgel terhelt módon jelenik meg a közbeszédben és a médiában.

Márpedig az internethasználók hálózati aktivitásának pragmatikus és elvi megítélése pontosan ilyen: erős vitatérben, érzelmi szélsőségektől sem mentesen formálódó diskurzus, ahol a személyes tapasztalatok és a személyes érintettség gyakorta csap át túlzó általánosításba. Tibi bácsi állítása egyetemlegesen vonatkozik valamennyi netezőre. Ha meginterjúvolhatnánk a tárgyban, bizonyára elfogadná sajátjaként azt az értelmezést: vannak olyan hálózati polgárok, akik az arctalanság védőernyője alatt másokat bántó közlemények megfogalmazásában jeleskednek, és közöttük találjuk mindazoknak a még szűkebb részhalmozát, akik egyenesen vele foglalkoznak.

A (talán jogos) indulat nem hitelesítheti azonban a túlzást: minden netező sunyi, társadalomképtelen alak volna. Ne felejtjük el, hogy amikor az ismert rádiós ezt nyilatkozta – 2002. június 26-án –, Magyarországon még többen voltak azok, akiknek nem lehetett közvetlen tapasztalatuk az internet-szubkultúra természetrajzáról, akik ismereteiket közvetett forrásokból szerezték. Ha közülük bárki hajlott arra, hogy elítélően bélyegezze meg a netezők számára furcsa és érthetetlen világát, akkor könnyűszerrel olvashatta nézetei erőteljes megerősítéseként, egy tekintélyszemély által hitelesített argumentumként az inkriminált sorokat.

„Minden könyv felkerül a torrentoldalakra”¹ – találta mondani a Google kipellengérezése közben Matyi Dezső, az Alexandra Kiadó tulajdonosa a Könyvfesztivál egyik előadásán. Ezt azzal illusztrálta, hogy saját toplistájuk első tizenöt helyezettjéből a cég informatikusa negyedóra alatt tizenkettőt megtalált magyarul a neten. Nagy kérdés, miért nem elégedett meg azzal, hogy úgy fogalmazzon: „legnépszerűbb könyveink nagyobb része sajnos elérhető kalózmásolatban a magyar weben”, hiszen mondata második felével pontosan azt bizonyította be, hogy még saját toplistájuknak sem minden darabjára igaz az állítása.² (Hát még az összes többi könyvre, amelyik éppen nem letölthető. Mindenna-

pi tapasztalatunk az, hogy a keresett tételek nagyobbik részéről mondható el: „még nem érhető el”).

Később Matyi Dezső így fogalmazott: „mindenki feltehet mindent a netre” – látszólag elfeledve azt a különbséget, hogy amikor a tényleges kalózkodás bekövetkezik, addigra a mindenből valaki lesz, a mindenből valami. Elfeledve, hogy elsőprő többségben vannak a nethasználók között azok, akik soha nem tesznek közzé illegális tartalmat, és a könnyűszerrel elérhető tartalmak világát messze meghaladó Deep Webhez³ képest is elképesztő méretű a meg nem osztott tartalom.

Figyeljük meg a következő, Horváth István Sándortól származó levezetést, amely az *Új Ember* című újság portáljának egyik számában volt olvasható:

„Személyesen tapasztaltam, hogy ottlétem alatt a háttérben osztálytársával chatelő fiatal semmilyen érdemi információt nem kapott és nem is küldött. A párbeszéd színes hangulatjelekből és azok cserélgetéséből állt; és itt vannak a jelentős időt lefoglaló játékok is, virtuális eszközökkel, virtuális vagy néha valós, de ismeretlen játszótárral... Megállapíthatjuk, hogy az internetes időtöltés semmivel sem tartalmasabb vagy hasznosabb a fiatalok számára, mint a televíziózás”.

Ugye feltűnő, hogy a szerző az internetes időtöltés hasznosságára vonatkozóan mindössze kétfajta tevékenység – az osztálytársakkal való chatelés és a számára „üres” stratégiai játékok – alapján von le általános következtetést? Hogy a fiatalok chatelési szokásainak azáltal vált „szakértőjévé”, hogy egy alkalommal részese volt egy hangulatjel-cserélgető párbeszédnek? Bizonyára nagyon meglepődne az internetezést haszontalannak és tartalmatlannak tartó szerző, amikor az internetkutatók empirikus adataival szembesülve kiderülne számára, hogy a többi, általa nem említett tevékenység – például tanulás, hasznos információk keresése a neten, közös felkészülés egy csoportos munka teljesítésére – milyen sok helyet foglal le a diákok időháztartásában, vagy hogy az

emotikonok⁴ információcsere nélkülinek gondolt küldözgetése valójában milyen sok tartalmat, jelentést és funkciót hordoz.

A lóláb persze kilóg! Látszik, hogy az idézett szerző ítélete már a kérdés vizsgálata előtt készen állt: az internetezés a szintén „haszontalan” tévőzéshez hasonlóan passzív, cselekvést nem igénylő időtöltés. Ezért a valóságot igyekezett hozzáigazítani a saját, arról alkotott képéhez. A nagy gond az, hogy a kérdés tárgyalása a pusztá logikai szerkezet miatt autentikusnak tűnhet. Igazoltnak látszó (valójában téves és esetleges) argumentumok megjelenítése után jutunk el a nagyívű, általános, univerzális következtetéshez, amely már köszönőviszonyban sincs a valósággal. Nem feledkezhetünk meg arról, hogy mindez egy erős bizalmi mezővel jellemezhető olvasótábor számára íródott, akiknek nem a kritikai pozíció az elsődleges befogadói parancs, különösen akkor nem, ha egyébként ők maguk is osztják az idézett szerző kiindulópontjait.

Az internetkutatók legalább tizenöt éve próbálják nyesegetni a felszínes leegyszerűsítések és merész általánosítások világának a fentiekre emlékeztető extrém szélsőségeit, sokszor eredménytelenül. Sajnos gyakorta előfordul, hogy maguk a tudóstársak, a kutatók is érzéketlenek a finom modalitásokra, és szakmai standardjaiknak komoly engedményeket téve állampolgári, szülői vagy más félelmeiket vetítik bele az aktuálisan tárgyalt témakörbe. Márpedig a „kínálat” óriási. Az internet veszélyei között megtalálható a hálózati szenvedélybetegség, játékfüggőség (lásd Demetrovics Zsolt és Koronczai Beatrix kötetünkben közölt írását), erőszakhoz kapcsolódó szubkultúrák (bombagyártás, iskolai mészárlások, mások nyilvános gyalázása, *cyber-bullying*),⁵ pedofília és szexuális ragadozók a neten, pornográfia, eltunyulás, elsivárosodás. Mindez bővül a kiberbűnözés sok formájával: adat- és identitáslopás, adathalászat, spamtek, hoaxok⁶ (lásd Talyigás Anikó fejezetét), a forgalom megbénítása, illegális adatcsere, adatpusztítás (cracking). Különös izgalmat keltenek a megfigyelés és az ellenőrzés veszélyei (lásd Székely Iván fejezetét).

Éppen a „forró” témáknak ez a formagazdagsága a különös ok, amiért megkülönböztetetten fontos, hogy ne csak a tárgyi tévedésekre, hanem a nyilvánosan megjelenő állítások pontosságára is érzékenyek legyünk.

Emberek és kvantorok

A természetes nyelv bizonytalanságainak kiküszöbölésére (is) vállalkozó logikában két világ, két, egymástól mély szakadékkal elválasztott állítástípus létezik:

1. a „minden x -re igaz, hogy...” típusú formula (az ún. univerzális kvantor), és

2. a „van olyan y , amelyre igaz, hogy...” formula (amelyet egzisztenciális kvantornak neveznek).

A logikai szabályok hasznosak az állítások igazságtartalmának eldöntésekor, ha adott formára tudjuk hozni őket. Abban a pillanatban, hogy akárcsak egyetlen x -et is találunk, amelyre nem igaz az állításunk, az univerzális kvantor érvényét veszti.⁷ Ilyenkor a kutató nem tehet mást, mint hogy pontosan jelzi, mennyire diszkontált az univerzális kvantor. (Egy kivétellel valamennyi x -re igaz, hogy... Majdnem minden x -re igaz, hogy... Az x -ek túlnyomó részére igaz, hogy... Az x -ek nagyobbik részére igaz, hogy...)

Vagy vegyük az állítások modalitásait, vagyis azokat a vonatkozásokat, amelyekben értelmezhetők és értelmezendők. Amikor egy jelenséget írunk le, különlegesen fontos, hogy pontosan abban a keretben beszéljünk róla, ameddig ismereteink és a választott tárgyalási mód engedik. Lehetséges vagy valóságosan jelenlévő? Szükségszerű? Esetleges? Általános? Jellemző? Kivételes? Domináns?

Ebből a szempontból tipikusnak tekinthető a korszerű technika és ezen belül a videokamerák felszereléséből adódó „megfigyelhetőség”-diskurzus körüli pongyolaság. A megfigyelhetőséggel riogatók szeretnek úgy tenni, mintha a megfigyelés lehetősége azonos volna a tényleges megfigyeléssel és megfigyeltséggel.

Arról nem is beszélve, hogy a rendszerbe állított kamerák képe túlnyomórészt csak videojelet rögzít, tényleges megfigyelés akkor lesz belőle, amikor a felvétel megtekintése valamely oknál fogva szükségessé válik. A felháborodók számára is vannak olyan szeletei ennek az univerzumnak, ahol egyetértésükkel találkoznak ezek a megoldások, mert az ő érdekeiket szolgálják. A létező gyakorlatoknak és a mögötte álló funkcióknak az orwelli⁸ anti-utópiákkal⁹ való összecsúsztatása már eddig is nagyon sok kárt okozott, és jócskán nehezíti a tisztánlátást.

Az effajta különbségek érzékeltetése a tudós számára alapvető kötelesség, hiszen ellentmondásmentes kifejtésre kell törekednie. Leginkább talán a sajtónyelv az, ahol a szerkesztők és az újságírók a figyelemfelkelés imperatívusza miatt gyakran érzékeltenné válnak az árnyalatok pontosságára.

Néhány az ijesztő példák közül: *A számítógép kövérré és nem-törődömmé tesz?* – kérdezi a Terminal.hu¹⁰ 2009. májusi cikkében egy brit kutatásra reflektálva Szilágyi Szabolcs felelős szerkesztő. Mutassunk fel egyetlen nem kövér és nem nemtörődöm számítógép-használót, és máris kiderül, hogy értelmetlen az univerzális kvantor használata.

De az igazi gondok csak ezután jönnek. Nézzük, milyen szerkezetben jelennek meg az ismert agykutató, Susan Greenfield¹¹ által irányított kutatás eredményei egy ismeretterjesztő cikkben. A játékosok túlzott monitorbámulásának „bőjtje” az, hogy „túl-ságosan sokat esznek, és a mozgásszegény életmód miatt hamar elhízhatnak”. Mivel a valósággal ellentétben nem kell tartaniuk a negatív következményektől, mint a fáramászás esetében a leeséstől, kevésbé lesz aktív az egyik legfontosabb agykérgi területük, az ún. prefrontális lebeny (és minél kövérebb valaki, annál kevésbé). Mindezek együtt „a koncentráló-készség csökkenéséhez, érzelmi sivársághoz és a képzelőerő elsorvadásához” vezetnek. Következtetés: „a számítógépek káros hatással vannak az életünkre.”

Ez a levezetés szomorú és kimeríthetetlen „kincsesbányája” a tévedések, pontatlanságok és felületességek világának, amelyek veszélyeire nem lehet eléggé figyelmeztetni.

Miközben az „emberekről” és az „életünkéről” szólnak az univerzális következtetések, a vizsgált célcsoport: a „számítógépes játékot játszó” – feltehetően fiatalokból álló – ismeretlen méretű minta. Kimondható: semmiképpen sem mindenki, még ha közülük sokan játszanak is, de nem igaz rájuk a „túlzott monitorhasználat”. Végül még a „túlzott monitorhasználók” közül sem mindenki kövér. Feltehetően az átlagtól valóban ebbe az irányba térnek el az idetartozók, de hogy mekkora mértékben, azt alapos vizsgálatokkal lehetne kideríteni (már ha ennek volna egyáltalán értelme).

Továbbá: egyetlen fajta felhasználása a számítógépnek (a játék) azonosíttatik a számítógép teljes hatásspektrumával. Egyetlen területen levont (amúgy, mint láttuk, sokszorosán helytelen) következtetés a teljes számítógépes univerzumról mond megfélebbíthatatlannak tűnő ítéletet. Vegyük észre: az „érzelmi sivárság és a képzelőerő elsorvadása” is abszolút minőségek, a használt fordulat még arra sem ügyel, hogy ennek valamilyen mértékére vonatkozóan állítson valamit.

Ha át kellene fogalmaznunk a kutatás eredményeit, valahogy ekképpen kellene: a számítógép-használók csoportján belül intenzív játéktevékenységet folytatók közül bizonyos játékokkal más tevékenységek rovására túlzottan sokat foglalkozók némelyikére veszélyként leselkedik az elhízás és a kockázatkezelésért felelős agyterület alacsonyabb aktivitása.

Az érintettek közül a leginkább veszélyeztetettekre jellemző lehet az, hogy érzékelhető csökkenést tapasztalunk a koncentrációképességükben és képzelőerejükben, ami együtt járhat az érzelmi elszárossodás bizonyos tüneteivel.

Micsoda beláthatatlan távolságig jutottunk a magabiztos végkövetkeztetéstől (a számítógépek káros hatással vannak az életünkre)!¹² Sajnos Rejtő Jenő¹³ elhíresült szállóigéjének mintájára – nem állíthatunk minden pofon mellé egy közlekedési rendőrt – azt kell mondanunk: nem állíthatunk minden módszertani és logikai hibáktól hemzsegő szöveg mellé egy tárgyilagos és felkészült tartalomelemzőt. Pedig elkelne, mert akad itt még más is.

Fantompozíciók kritikája, avagy a Morozov-effektus

Jevgenyij Morozov a washingtoni Georgetown Egyetem patinás intézetének (Institute for the Study of Diplomacy) kutatója, a *Foreign Policy* című szaklap NetEffect Blogjának szerzője. Ilyen kiváló pedigrével egyenesen szégyen, hogy milyen nemtelen érvelés-technikai megoldásokkal élt 2010. áprilisi (majd májusban és júniusban is javított), nagy port felverő vitáirátának elkészítésekor.

A rövid esszé azt igyekszik bizonyítani, hogy a web korai rajongói által megjósolt kiber-utópia egyre illuzórikusabbnak látszik, mert a való világban semmi nem változott.

Az ehhez választott módszer egy mesteri fokra fejlesztett dupla érvelési csalás: nagyságrendekkel eltúlozni, amit néhány egykori gondolkodó állított, majd egy-két, mindennek látszatra elmentmondó jelenséggel bebizonyítani, hogy nem volt igazuk.

Hogyan működik ez a technika? Nicholas Negroponte,¹⁴ az MIT MediaLab legendás vezetője 1997-ben azt jósolta: a nemzetek közötti határok leomlásával a világbéke új korszaka érkezik el, a „másik” országokhoz az internet nyújtotta közvetlenséggel és személyességgel közeledő, a nacionalizmust már hírből sem ismerő fiatalokkal.¹⁵

Morozovnál ebből csak az „örök béke” (*perpetual peace*) ígérete lesz. Ha Esther Dyson és Alvin Toffler híres manifestuma, a *Magna Charta for the Knowledge Age*¹⁶ 1994-ben az „elektronikus szomszédság” előretörését jósolja,¹⁷ akkor Morozov ebből csakis olyan közösségeket lát és kér számon, amelyek „rosszabbá teszik a világot”: védett állatok kereskedelmére az interneten szövetkező gonoszokat vagy homofób tüntetésüket online szervező szerbiai szélsőségeseket. E két példa már elég is neki, hogy kimondja: a világ nem lett igazságosabb az internet által, nem hozta el a globális béke, szeretet és szabadság korszakát („we haven’t seen an Internet-powered rise in global peace, love and liberty”). Nem buktatta meg továbbá a diktátorokat, nem lettek elszámoltathatóbbak a kormányzatok, nem nőtt meg a politikai folyamatok alakításában résztvevők száma – egészíti ki a listát a blogger.

Nehéz megállni, hogy ne olvassuk az idézett szerző fejére: továbbá az internet nem fogyasztotta le a kövéreket, nem szépítette meg a csúnyákat, és nem gazdagította meg a szegényeket. Ezeket ugyanúgy nem várta és nem is ígérte senki a nagyjából tizenöt évnyi kis hálózattörténet után, mint a Morozov által citált dolgokat.

Az említett szerzők trendeket, mozgásirányokat igyekeztek azonosítani, amelyek lassan átalakítanak majd működésmódokat. Előrejelzéseik az internetben rejlő potenciál kibontakozásáról szóltak, olyan tendenciákról, amelyek máris érzékelhetők, adott irányú változásuk feltételezhető, és beleilleszthetők bizonyos logikai szerkezetekbe (ha egy adott jellegzetesség adott irányba változik, várhatóan adott irányba fog elmozdulni egy másik jellegzetesség is). Fokozatosan kibomló, egymással ellentétes folyamatokat egyidejűleg produkáló, összetett problémákról van szó. Főlöszeges és félrevezető pozíció valamilyen állapotot számon kérni akkor, amikor a változás finomszerkezete a kérdés. Egy olyan jelenségvilágból pedig, amelyik hihetetlenül sokrétű, ezerféle történeten keresztül leírható és megérthető, egy-két egyoldalúan kiragadott sztoriból univerzális állításokig jutni alapfokú oktatási intézményekben is bukást jelentő szellemi tett lenne, nemhogy nagy olvasottságú online orgánumban.

A lóláb kilóg! – mondhatjuk megint, mivel az említett szerző az internetkutatók diskurzusában nem tud megjelenni, mert nincs hozzá gondolata és elég ismerete. Publicistaként a zsigeri „internetellenesek” „na végre megint valaki jól megmondta azoknak a netprófétáknak” típusú, talmi igényeinek kielégítésére vállalkozik. Nem kell csodálkozni, hogy rajongó hozzászólói ilyen színvonalú, a sokszorosán megcáfolt hálózati folklórból jól ismert kommentárokkal dicsérik: „Egyet kell értenem. Az internet kb. 50%-a a pornóról szól. A másik fele sem sokkal kevésbé furcsa.” És ha ezt a fajta blödlit már Morozov sem vállalná, azért valaki figyelmeztethetné: nagyban hozzájárult ahhoz, hogy körmönfont ostobaságok narratívaképző fordulatként keringhetnek a közgondolkodásban.

Következtetési (optikai) csal(ód)ás

„Minél többet iszom, annál jobban remeg a kezem. Minél jobban remeg a kezem, annál többet lötytyintek ki az asztalra. Minél többet lötytyintek az asztalra, annál kevesebbet iszom. Tehát: minél többet iszom, annál kevesebbet iszom.”

Sokan ismerhetik ezt a tréfás, becsapós levezetést, és bizony nem is keveseknek gyűlik meg vele a bajuk, hogy megtalálják a „kegyes csalás” hatásmechanizmusát. Pedig ez fontos képesség, aminek jó hasznát vesszük akkor, amikor ilyen állítással találkozunk: „Minél több folyóirat érhető el online, annál kevesebb ezekben publikált cikkekre hivatkoznak a tudományos kutatások referencialistáiban.” Neville Holmes írásában furcsa tételt állít fel számunkra. Pusztán attól, hogy széles körben elérhetővé váltak a szakfolyóiratok a weben, csökkenésnek indult a hivatkozások száma (ami baljósan hangzik a szellemi termelés jövője szempontjából). Holmes feltehetően nem erre gondol, csak gondatlanul fogalmaz. A problémát minden bizonnyal a tanulmányokat közlő online szakfolyóiratok számának meredek gyarapodásában látja, azt sugallva, hogy a közölt szakszövegek mennyiségnövekedését nem követi a tartalmakra fordított, hivatkozásszaporításban tetten érhető figyelem. Másképpen: a felhasználás elmarad a gyártástól, és ez sötét árnyékot borít az ismerettermelés és -fogyasztás jövőjére.

Jellemző, hogy egy több évszázados, számtalanszor megcáfolt közhely (ti. hogy belefulladunk saját szövegtermelésünkbe) újracsomagolt változata két sorban megfogalmazható, de hibáira, csúsztatásaira, végiggondolatlanságára sok-sok bekezdést kell szentelnünk, hogy egyértelmű és világos legyen, mi a baj.

Először is nem derül ki: Holmes abszolút számokra, vagy arányokra gondol? Bármelyikről van is szó, hol vannak mögüle az adatok? Úgy tünteti fel továbbá, mintha a kvázi-egyenletnek pusztán két eleme (oldala) volna, a folyóiratszám és a hivatkozás. Valójában azonban négy eleme van:

- új tudományos tartalmak létrehozása;
- ezek megjelenésének, publikációjának, közzétételének jellegzetességei ;
- a nyilvánossá lett tudományos szövegek fogyasztásának, hasznosulásának, továbbélésének kérdései;
- és végül a tartalmak hivatkozások formájában mérhető értékelése.

Ugye azonnal fel is ismerjük a csalafintaságok első rétegét? A hivatkozások számának követésével nem azt mérjük, hogy volt-e értelme létrehozni egy adott közleményt, hogy azt használta-e valaki (egy tudományos szöveg számtalan formában hasznosulhat másképpen is).¹⁸ A hivatkozásmérés korlátozottan és alkalmilag a tudományos teljesítmény elfogadottságára, a szerzők presztízisére, ismertségére vonatkozó állításokhoz használható.

Valószínűleg senki sem vitatja azt, hogy a tudomány és a megoldásra váró problémák természeténél fogva a közlemények formájában megjelenő új tudás minél nagyobb mennyisége kívánatos. Ehhez a közleményeket létrehozók számának növekedése és/vagy a szerzők nagyobb termékenysége, tanulmányírási hajlandósága egyaránt hozzájárulhat. Az az igény, hogy szülessen kevesebb, publikációban testet ültő új tudás azért, hogy ne csökkenjen az egy közzétett tudáselemre eső hivatkozások száma, semmiképpen sem írhatja felül az új tudások minél nagyobb mennyiségben való létrehozásának imperatívuszát.

Ez az a pont, ahol Holmes – ha módot adnánk rá – feltehetően úgy pontosítaná tézisé, hogy ő a hivatkozások csökkenésén keresztül valójában csak a tudományos közleményeknek a gyarapodással párhuzamos minőségromlására igyekezett felhívni a figyelmet. (Amiből egyenesen következne az a nélkülözhetetlen előfeltevés, hogy a hagyományos, nyomtatott csatornákat megkerülő online szakmai publikációk pusztán a közlés módja miatt alacsonyabb értékűek lennének. Ennek bizonyításával a szerző adósunk marad.)

De itt még nincs vége. Mi történik azzal, hogy szaporodik az online formában (is) elérhető folyóiratok száma? Milyen jelen-

ség áll emögött? Alapvetően két felhajtóerőt látunk mozgásba lépni. A zárt, nagy presztízsű, profitelven működő, és ezzel párhuzamosan korlátozott közleményfelvevő képességű folyóiratok „elitvilága” mellé alternatív felületek létrehozását (hogy több és korlátlanul hozzáférhető szöveg jelenhessen meg), másrészt a tudomány kohójában állandóan újraformálódó tudományközi határok, tématerületek, megközelítésmódok, módszertanok által szakadatlanul igényelt specializációt, amellyel egy-egy szűkebb, frissen kialakuló „emergens” (kibontakozó) téma művelői számára biztosíthatók a közös gondolkodás szakosított keretei. Ismételten azt kell mondanunk, hogy mindkét irány sokkal erősebb és fontosabb annál, semhogy mondvacsinált és bizonytalan minőségi fenntartások miatt megkérdőjelezzük a létjogosultságát. (A „hogyanról” természetesen lehet és kell is beszélni, alapos ismeretek és kiérlelt megfontolások alapján).

És ne higgyük azt, hogy a felületesség és a megtévesztés bajnokainak nem marad hova visszavonulniuk a fals érvelések beszorkánykonyhájából.

Szóhasználat

Nem meglepő, hogy sokszor azok a kifejezések, amelyeket egy jelenség leírásakor használunk (anélkül, hogy logikai szerkezetekbe helyeznénk őket), pusztán szóhangulatuknál fogva is eltérítetik a tárgyilagos értelmezést, mert már kiválasztásuk is a befogadónak az adott prekonceptió felé való hajlítását szolgálja.

Az ámokfutó tinédzserek családi-magánéleti háttérét fürkésző írások nem mulasztották el következetesen „öldöklős programoknak” nevezni azokat a játékokat, amelyekkel a fiatalok szívesen töltötték az időt, rájátszva arra az ostoba és hamis előfeltevésre, hogy mindennek köze volt a szörnyű tettehez. (A leggyakrabban használt „lövöldözős játék” már egy fokkal semlegesebb kifejezés a természetüket tekintve a reflexjátékok közé tartozó programokra.)

Hasonlóképpen igyekszik olykor a szótárba a „szörny”, hogy bizonyos játéktípusok diabolizálásával azok „szörnyű” tartalmát, a szerzők elrettentő üzenetét erősítse. Mindez a Pokémon-kultusz¹⁹ idején ért zenitjére, amikor e kedves, szerethető lényeket a szó eredetére utalva rendszeresen „leszörnyezték” a szorgos tollforgatók. Amikor minden „online pornó”, akkor bármilyen elemzés alkalmatlanná válik a hálózaton megjelenő egészséges erotika és a deviáns szexualitás eltérő tárgyalására. Azon már nem is lepődünk meg, hogy a rosszindulatú netes károkozóból, a pusztítási szándékkal tevékenykedő crackerből rendszeresen hacker lesz a híradásokban. Hiába mondja, meséli, definiálja „szét” a szakma a két kifejezést, szinte lehetetlen elérni, hogy a megfelelő helyzetben a megfelelő formulát használják (lásd erről könyvünkben Rácz Bencze írását.)

A hamis tudattól a morális pánikig – miért kártékonyak az inkorrektén érvelő szövegek?

A fentiek nyomán jól látható, hogy sok esetben következetes és hosszabb ideig folytatott tisztítókúrára van szükség, hogy végre adekvát problémaszervezetben vizsgálhassuk Digitália valóban lényeges kérdéseit. A kiválasztott példák alapján eddig megjelent problémákat befejezésül tehát pontokba szedve összefoglaljuk, majd röviden értékeljük a morális pánik kialakulásában játszott szerepüket.

Az állampolgári, a média- és a tudományos diskurzusok összecsúsznak:

- A gyakorta kontextus nélküli, hibás általánosításra épülő kiinduló állítások előszeretettel szaladnak öngerjesztő következtetési spirálba.

- Azzal, ahogyan oksági elemzés helyett „közkeletű képek” formálják a tárgyalást, az érvelési hibára épülő szövegek nem a vizsgált rendszer jobb megértésének irányában fejtenek ki nyomást, hanem magának a lehetséges vizsgálatoknak az ismeretelméleti szerkezetét torzítják morális és ideológiai görbe tükörrel.

– Ezzel valójában pótcselekvés ment végbe, elhozva a talmi megnyugvást. A probléma szerkezete viszont nem változott, és a valódi gondok orvosolatlanok maradtak.

– A rossz elemzésekből felépülő, szempontokat onnan merítő véleményekből kiindulva szinte csakis helytelen elemzések és értékelések születhetnek egy adott kérdéskörrel kapcsolatban, azok pedig egyenesen vezetnek rossz döntésekhez és az azokból következő inadekvát beavatkozásokhoz.²⁰

A társadalmi párbeszéd argumentációs bázisa leszűkül, a racionális kommunikáció esélyei csökkennek. A percepciók, jelentések és értelmezések cseréje lelassul, a másfajta megközelítésekhez nehezebben teremthető viszony.

Lehetséges veszélyforgatókönyvek (általában jól ismert anti-utópia-készletből válogatva) faktuális tényként jelennek meg.

Mivel a fentiekből fakadóan a veszélymodalitások és az érintheztség mértékének megjelenítése folyamatosan felfelé térítenek el a valóságtól, ez megfelelő táptalajt kínál a pusztító morális pánik kialakulásához.

Morális pánikjelenségek (amikor az ismeretlen és felforgató „új” értékvesztésként és a mindennapi élet megszokott szerkezeteit veszélyeztető módon jelenik meg a nyilvánosság fórumain és a közösségek információs áramlásrendszerében) minden jelentősebb technológiai váltás környékén kialakultak. Nem csoda, hogy „dramaturgiáját” tekintve most is ugyanúgy játszódik le minden, ahogy korábban is szokott: Egy deviánsnak minősített aktussal, történéssel kezdődik, amely egyediségéből kiszakítva válik médiatartalommal, a megjelenítés felszínessége miatt azonnal egy általános, fenyegető trend részeként.²¹ Emiatt még az önmagukban elhanyagolható esetek jelentősége is megnövekszik, és nincs, ami ellensúlyozza az egyoldalú feldolgozást. Az ellenpéldák ismeretlenek maradnak vagy súlytalanná válnak, hiszen médiatartalomként nem annyira „érdekeselek”, és könnyű figyelmen kívül hagyni őket, ha nem illenek bele a kialakult sémavilágba. A hírek forrásai általában érzéketlenek a teljes kontextusra, kiragadott részletek alapján, „egydimenziósan” ítélik meg, így épül-

nek egy pillanat alatt az egyes olvasói rettegésekből diadalmas univerzális narratívák.

Amikor önálló életre kel egy-egy pánikdiskurzus, már nagyon nehéz azt megállítani. Szülők, tanárok, politikusok a „felelősség-szerep” miatt ráadásul óhatatlanul szinte automatikusan az óvatos elfogadás felé hajlanak. Kisebb hibának tűnnek ugyanis a veszélyek esetleges túlértékeléséből fakadó következmények, az elmaradt hasznok, mint az alulértékelés lehetősége miatt elmulasztott beavatkozások kockázatai és „költségei”. Ez az oka annak is, hogy a pánikdiskurzus nyomása sokszor olyan erős, hogy az elfogadott vélekedések gyakorta „felülírják” a saját, személyes tapasztalatokat is. Könnyebb azt gondolni ilyenkor, hogy „bizonyára én tévedek”, „biztos azoknak van igazuk, akik nálam jobban értenek a dologhoz”, mint vállalni a saját, a közvélekedéstől eltérő álláspontokat.

2009 tavaszán egy igényes gyermeklapba írtam a számítógéphasználatról egy rövid cikket,²² amelyet legnagyobb örömömre sok iskolában használtak fel a tanárok a témáról való beszélgetés kezdeményezésére, illetve szövegértési és -értelmezési nyersanyagként. A gyerekek által készített vélemények közül aztán számos váci és szegedi kisiskolás hosszabb-rövidebb fogalmazása el is jutott hozzám. Miközben boldogan olvastam a 9-10 évesek gondolatait, megrázó volt ráismerni a sorok között és mögött a tekintélyszemélyek, a tanárok és szülők által közvetített pánikdiskurzusokra. Előbb-utóbb mindenki elmesélte, miért szereti, mire használja a számítógépét, miért jó neki, de előtte kötelességszerűen „felmondta” a leckét, hogy milyen egészségtelen, mennyire rontja a szemet és a gerincet, hogy elhízáshoz vezet. Különösen beszédes volt annak a kisfiúnak a vallomása, aki az első oldalon kifejtette, hogy a számítógépezés a tanulás rovására megy, majd büszkén és átmenet nélkül számolt be róla a második oldalon, milyen jól tudja felhasználni a gépet iskolai feladatai teljesítéséhez, és mennyi hasznos dolgot talál az interneten a maga számára.

Cseppnyi kétségünk se legyen: már a 8–12 éves korosztály tagjai is teljes mértékben alkalmasak és méltók arra, hogy a számítógépes kultúra alapkérdéseivel megfelelő szerkezetben és mo-

rális pániktól mentesen, a rájuk leselkedő veszélyek valóságos természetének megfelelően ismerkedhessenek meg. Ne felejtjük el: valamennyien „digitális bevándorlók” vagyunk, emiatt mindekelőtt igencsak alaposan meg kell ismerni annak a világnak a törvényszerűségeit és jellegzetességeit, amely a „digitális bennszülöttek” természetes közege.²³ Különösen igaz ez, ha mi kívánunk eligazítással, iránymutatással, netán tiltással vagy ajánlással élni ezt a világot érintően. Ugyanez az óvatosság és felkészültség nem árt, ha különböző digitális bevándorlók (szülők, családtagok, pedagógusok, újságírók, kutatók) egymás között szeretnék tisztázni a számukra fontos alapkérdéseket e témakörben.

Talyigás Anikó *A Madách Imre Gimnázium
matematika–informatika szakos tanára 2002 szeptem-
berek óta*

AZ INFORMATIKAOKTATÁS DINAMIKÁJA¹

A következőkben szeretném megosztani az olvasóval az informatika tanítása során szerzett tapasztalataimat. Először a tantárgy változásairól és a tantervi elvárásokról, majd az érettségi és a tanítás kapcsolatáról szólok. Írok néhány szót az internet veszélyeiről az informatikaórán és azon kívül. Majd megismertetek az olvasókkal egy, az internet veszélyeire és lehetőségeire felhívó órasorozatot, amelynek eredményeiből, azaz a gyerekek írásaiból is olvashatnak idézeteket. Végül példákat mutatok az internet iskolán belüli, informatikaórán kívüli hasznairól. A tanulmányomban leírt személyes tapasztalatok nem általánosíthatók, egy-egy iskolára korlátozódnak.

Tanterv

Nincs még egy olyan tantárgy, amely annyit változott és fejlődött volna tíz év alatt, mint az informatika. Amikor 1999-ben elkezdtem Újpesten tanítani, még a DOS operációs rendszert és a Win-

dows 3.1 segédprogramot tanítottuk a gyerekeknek, és akkoriban az internetről igen kevés szó esett az órákon. Az iskolának még nem volt internetes kapcsolata, a gyerekek nagy részének számítógépe sem volt otthon.

2002-ben kezdtem tanítani a fővárosi Madách Imre Gimnáziumban. A beadandó házi feladatoknál kiderült, hogy voltak olyanok, akiknek nem volt számítógépük, és sokan nem tudtak feljelentkezni az internetre. Még a 2004/2005-ös tanévben is érkeztek gyerekek, akik az általános iskolában nem tanultak számítástechnikát, de voltak velük egy csoportban olyanok is, akik már több ECDL-modult² letettek. A gimnáziumba kerülő gyerekek informatikai tudása között ma még mindig nagyon nagy különbségek vannak, de már sokkal kevésbé merül fel, hogy valaki ne tudna otthon számítógéppel házi feladatot készíteni. A gimnáziumot most kezdő tanulók megközelítőleg 90%-ának az internet használata mindennapi élete részévé vált.

A normál tantervű gimnáziumokban 2008-ig, de vannak iskolák, ahol még most is két évig heti egy, vagy egy évig heti két informatikaóra jut a négy évre. A két verzió közül talán még mindig a második a kellemesebb, hiszen heti egy órában nagyon nehéz teljesíteni a tantervi követelményeket. Szerencsésebb esetben tehát évi 72 órában ismertetjük meg a tanulókkal az operációs rendszer használatát, a szövegszerkesztést, a táblázatkezelést, a prezentációkészítést, a weblapkészítést és az adatbázis-kezelést. A szoftverek alkalmazásának mélysége függ a csoporttól, a kezdés lehetséges szintjétől. Ezek mellett azonban egyre inkább teret kellene kapniuk az internettel kapcsolatos ismereteknek.

Az internetes ismeretek egy része beépíthető más szoftverek tanításába, emellett a többi szaktanár feladata lehet, hogy adjanak olyan feladatokat a gyerekeknek, ahol böngészniük kell az interneten található információrengetegben. Ezeknél a feladatoknál elsősorban az interneten való keresést, a megtalált adatok másolását, mentését tanulhatják meg a diákok.

Például ha egy filmekről szóló táblázatot készítünk az Excel program segítségével, akkor kapnak egy kis időt, hogy két-há-

rom sort önállóan töltsenek fel olyan filmekkel, amelyeket szeretnek, és a szükséges adatokat az interneten kereshetik meg.

Amikor először adtam ilyen feladatot, a gyerekek nagyon örültek, annak is, hogy kedvükre tölthetik ki a táblázatot, és annak is, hogy használhatják az internetet. Az idén már kisebbnek éreztem az ilyen típusú feladatok adta örömet, hiszen az internet használatában a mai 14–16 évesek egyre kevésbé érzik az újdonság varázsát. A tanulók nagy része ma már úgy gondolja, hogy az internet terén nemigen lehet nekik újat mondani.

Azoknak a gyerekeknek a környezetében, akik most kerültek gimnáziumba, természetes az internet használata. Életük része, hogy társaikkal nem telefonon, hanem chaten kommunikálnak, hogy az osztálynak van honlapja, ahol az iskolával kapcsolatos híreket, képeket, érdekességeket osztják meg egymással és a világgal.

Megdöbbenve tapasztaltam ugyanakkor, hogy ez utóbbi megjegyzésem, amely szerint a világgal is megosztják a honlapon szerepeltetett gondolataikat, már nem természetes számukra. Voltak diákok, akik nem értették, miért szólok, hogy az osztály honlapján ne használjanak csúnya szavakat, hogy kérdezzék meg társaikat arról, hogy feltehetnek-e róluk képeket. Hasonlóan sokan nem gondolnak rá, hogy amit a jelenleg nagyon elterjedt közösségi portálokon írnak, azt minden „ismerős” látja. Így például ha szídnak valakit, akkor azt az érintett személy is olvashatja.

Fel sem merül bennük, hogy azt, amit egymásnak írnak nyilvános fórumokon, vagy azokat a képeket, amelyeket viccből feltesznek, bárki megnézheti. Miért baj ez? – kérdezheti az olvasó, és kérdezik a gyerekek is. A válasz nem olyan egyszerű, és azt gondolom, érdemes sokat beszélgetni erről a gyerekekkel. Szerencsére vagy nem, de nem merül fel bennük, hogy az emberek a feltett képeiket letölthetik, akár felhasználhatják montázsok vagy saját célra. Az sem jut eszükbe, hogy a házbulikról készült képeken nemcsak a mámoros barátok, hanem a család tévéje, számítógépe, lakásának értékei is láthatók, ami esetleg az adatlapokon feltüntetett címmel együtt már igencsak sok lehetőséget rejt magában a rossz szándékú keresőnek.

Érettségi

Fontosnak tartom, hogy idézzek az informatikai érettségi vizsga elvárásaiból. Ma a továbbtanulni kívánó gyerekek számára a legfontosabb kérdés, hogy mit vár el tőlük az érettségi. Az informatika érettségit a gyerekek általában már 10–11. osztályban „előrehozzák”, hiszen addig tanulják, addig frissebbek az ismereteik. Sok problémát felvet az előrehozott érettségi, hiszen tapasztalatom szerint a 16–17 évesek nagy része még nem érett a 15 perces folyékony szóbeli vizsgára, amelyben elvárják tőle az önálló fogalomhasználat, mondatépítés képességét. Másrészt ha a gyakorlati vizsga nem a számukra várt módon sikerül, egyszerűen megbuktatják magukat, nem mennek el a szóbelire, és a következő évben újra próbálkoznak. (Ha elmennének szóbelizni, már csak az iskola „jogi” falain kívül javíthatnák ki vizsgájukat.)

Ez az oka annak is, hogy az idei érettségin informatikából volt a legnagyobb a bukásarány.

Itt azonban nem az érettségi problémáit, hanem az internet adta lehetőségeket és kockázatokat fejtegetjük. Így most az érettségit is ezzel a szemmel vizsgálom. Mennyire kell tisztában lennie az internet veszélyeivel egy informatikából érettségiző diáknak? Mennyire kell tudnia tájékozódni az internet információs erdejében? Mennyire kell tudnia alkalmazni és ismerni az internet adta lehetőségeket, szolgáltatásokat?

Az informatikaérettségi két részből áll, egy 120 pontos gyakorlati és egy 30 pontos szóbeli részből. Az írásbeli rész a már feljebb felsorolt öt szoftver gyakorlati alkalmazását kéri számon. Az internetes ismeretek a szóbeli vizsga során kérhetők számon, hiszen gyakorlati vizsgán a vizsgázó nem használhatja a világhálót. Ez eleve azt jelenti, hogy e téren a számonkérés öt vagy hat tételben koncentrálódik a szóbelin húzható húsz tételből, hiszen a szóbeli vizsgán a tanulónak az informatika fejlődéstörténetétől kezdve az információ alapfogalmain (adat, jel, kommunikáció, információ) és mértékegységein keresztül többek között a hard-

ver- és szoftverismeretekről, szerzői jogokról, könyvtárismerekről is számot kell tudni adnia.

A szóbelin több témakörben is megtalálhatjuk érintőlegesen a kommunikációra, az internetre vonatkozó utalásokat, de „információs hálózati szolgáltatások” néven külön témakört is szentel a szóbeli elvárása az internetes ismereteknek.

A kompetenciáknál ezt olvashatjuk: „az informatika és a társadalom kölcsönhatásának felismerése (az informatika rohamos fejlődése az egész társadalmat gyökeresen átalakítja, s ebben az állandóan változó világban csak az érezheti otthon magát, aki érti a változásokat s azok mozgatóit).”

Az érettségi vizsga tartalmi része tizenegy témakörre bomlik. Ebből az információs társadalom és az információs hálózati szolgáltatások témakörökben találkozhatunk a világhálóval kapcsolatos utalásokkal. Az információs társadalomhoz tartozó részletezésben véleményem szerint elég általánosan vannak megfogalmazva az elvárások, így az internet érintőleges említésével is kidolgozhatók a témához tartozó tételek. A következőkben gondolhatunk arra, hogy a vizsgázónak mégis részletesebben kellene szóba hoznia a világhálót:

„1.2. Információ és társadalom – 1.2.3. Informatika és etika: Legyen elképzelése a legújabb információs és kommunikációs technológiák társadalmi hatásairól.

1.2.4. Jogi ismeretek – Ismerje a túlzott informatikai eszközhasználat személyiségromboló, egészségkárosító hatását. Ismerje a helyi és a távhálózatok netikettjét. Legyen tisztában azzal, hogy az adat, az információ áru, jelentős értéket képviselhet.”

Kifejezetten az internetre vonatkozó témakörben (7.1. Kommunikáció az interneten) elsősorban az elektronikus levelezés, a böngésző és a távoli adatbázisok használata mellett az interneten való keresésből kell elméletben és gyakorlatban számot adniuk a vizsgázóknak. Azt gondolom, középszinten elsősorban a felkészítő tanáron múlik, hogy mennyire kapnak hangsúlyt „a kockázatok és a mellékhatások”, illetve az előnyök és a lehetőségek. Amennyiben ilyen témájú tételt húz a vizsgázó, az elméleti be-

számolót (hogyan működik egy levelezőprogram, milyen funkciók állíthatók be; milyen lehetőségek vannak egy böngészőben, hogyan kereshetünk) egy, a tételben megfogalmazott gyakorlati feladattal kell kiegészítenie, amihez a teremben rendelkezésre áll egy internetre csatlakoztatott gép.

Összességében elmondható, hogy az érettségi elsősorban nem az internetes ismeretekre kíváncsi, hanem a tanult szoftverek alkalmazására helyezi a hangsúlyt.

Az érettségi elvárásai és a fent említett óraszámok ismeretében még egy problémát kell megemlítenem. Miért és mire tanítjuk, készítjük fel a gyerekeket? Azt gondolom, az életben való eligazodáshoz, a mindennapokhoz ma elengedhetetlen, hogy sokat tudjanak a gyerekek az információk kezeléséről, a megtalált információk hitelességéről, az általuk megadott adatok értékéről stb. Ha viszont azt mondja nekünk a tanuló, hogy érettségizni szeretne, akkor a tanár kötelessége, hogy a vizsgára készítse fel a tanulót.

Internet az órán és azon kívül

Egy másik aspektusból is gondot okozhat az informatikatanároknak és a rendszergazdáknak az internet léte. A diákok egy része ugyanis előszeretettel kezd el szörfözni a hálón, ha alkalma adódik rá. Ez több problémát is felvet. Talán a legkisebb ezek közül az, hogy az illető nem a tanórán kiadott feladattal foglalkozik, nem a táblázatot vagy a prezentációt készíti. Az is előfordul, hogy a tanár enged pár perc szabad foglalkozást, és ez idő alatt interneteznek a gyerekek. Kérdés, hogy a tanárnak van-e módja észrevenni, hogy éppen milyen oldalakat látogatnak ilyenkor a gyerekek. Találkozhatnak-e olyan tartalommal, amelyet általános vagy középiskolás tanulónak nem kellene olvasnia, nézegetnie, játszhatnak-e számukra ártalmas játékkal? Letölthetnek-e illegálisan zenéket, filmeket? Nézegethetik-e például az iskolai hálózaton elérhető képeket, és esetleg változtathatnak-e rajtuk?

Ezek a kérdések rögtön további kérdéseket vetnek fel, amelyek már nem csak az órai internetezés során okozhatnak bajt:

Tudja-e, hogy ha regisztrál egy oldalra, milyen adatokat adhat meg, kikkel kerül kapcsolatba?

Ha név nélkül fórumozik, chatel, tudja-e, kit rejtenek a nick-nevek?

Egy, az informatikatanárok által látogatott levelezőlistán is felmerült ez a téma. Az egyik tanár elmondott egy esetet, amikor egy ötödikes kislány társkereső oldalra jelentkezett be az iskolában (szabadidős foglalkozáson). Amikor a tanárnő meglátta, megijedt, gondolatban már a pedofília veszélyéig is eljutott, nem teljesen oktanul. Ő akkor kezelte a problémát, és elbeszélgetett a kislánnyal, de hogyan óvhatjuk meg ezeket a gyerekeket általánosan attól, hogy ártatlanul csapdákba lépjenek?

Előfordulhat tehát, hogy a gyerek kerül bajba, de az is, hogy a gyerek okoz kárt. A kérdés tehát, hogy hogyan védekezhetünk, hogyan óvhatjuk meg a gyerekeket? Hogyan vehetjük észre a veszélyt? Hogyan védekezhetünk ellene?

A levelezőlistán felvetett kérdésre több válasz is érkezett. Volt, aki azt mondta: ezek a problémák a tartalmak szűrésével védhető; volt, aki a házirend betartatását, illetve az internet letiltását tartotta biztos módszernek. A válaszok során néhány honlapot is ajánlottak a kollégák, amelyeken a veszélyekre felhívó gondolatokat találhatunk. Ezeket érdemes megnézni együtt a diákokkal, és megbeszélni velük, példákkal alátámasztani azokat. Ezeken a honlapokon találhatunk felhívást a vírusokra, a „csalilevelekre”, tippeket nyilvános helyen lévő gépek használatára, olvashatunk példákat arra, hogy kinek adhatja ki magát valaki egy társkereső vagy egy chat-oldalon.

Egy iskolai hálózatban megtehető, hogy

- az óra idejére letiltjuk a teljes internethasználatot (hálózatról függően gépenként vagy minden gépen);
- letiltunk bizonyos tartalmakat tartalmazó oldalakat;
- figyeljük egy külső gépen, hogy a tanulók éppen mit csinálnak, és ehhez megfelelő szoftverrel „belenyúlunk” a diák gépébe;

– megnézzük, miket töltött le, milyen fájlokat használt a diák.

A felsorolt lehetőségek sok jogi problémát is felvetnek. Van-e jogunk belenézni a gyerek által elmentett fájlokba? Van-e jogunk „belenyúlni” a gépébe?

Az internet egyre bővülő webhelyei miatt a letiltás sem egyszerű, állandó frissítéssel és odafigyeléssel sem szűrhetőek ki teljesen biztonságosan a káros webhelyek.

Én azt gondolom, hogy a szűrések is szükségesek, de igazi védelmet a megelőzés és a felvilágosítás nyújt. Időt és lehetőséget kell szentelni arra, hogy beszélgessünk a gyerekekkel a felmerülő veszélyekről, tájékoztassuk őket arról, hogy mire figyeljenek, és mit kell tenniük bizonyos esetekben.

Gyakorlati tapasztalat

Évről évre többet tudnak a diákok az internet kockázatairól, de épp amiatt, hogy ennyire az életük része lett, nagyon fontos feladatunknak tartom, hogy minél részletesebben tájékoztassuk őket a felmerülő veszélyekről és az internet adta lehetőségekről is.

Megkérdezem a diákokat, hogy ki szokott otthon számítógépezni. Általában maximum két ember nem teszi fel a kezét. Mit szoktatok a számítógépen csinálni? Értetlen tekintetekkel találkozom – hogyhogy mit? Hát internetezni. Értem, mondom, de mégis, ez mit jelent? A legtöbben egymással chatelnek, illetve a már említett közösségi portálokon keresnek ismerősöket az elmúlt tizenöt évükből, olvassák, hogy ki melyik alkalmazást használja, nézik ismerőseik és mások képeit, fórumbejegyzéseit. Kívülük vannak még olyanok, akik a manapság elterjedt játékokkal játszanak, stratégiai, illetve „ki lövi ki jobban egymást?” típusú játékokat. Meg kell jegyeznem, hogy a stratégiai játékok egy része sok szempontból hasznos, logikai képességeket fejlesztenek, rendszerszemléletet tanítanak. A számítógépes játékok használatának van egy határa, amin túl már felmerül a felhasználónál a függőség veszélye.

Tapasztalatom szerint mentalitás kérdése is, hogy valakit zavar-e, ha róla feltesznek képet, vagy hogy ő feltesz valakiről. Ezeknek a gyerekeknek természetes, hogy ha otthon ülnek, folyamatos információáradat éri őket a többiekről. Tudják, otthon vannak-e, vagy kimentek a vécére, tudják, épp melyik „alkalmazással” játszanak, illetve kinek lettek éppen az „ismerősei”. Nem gondolják és nem értik, hogy ez egészségtelen, hogy ez nem más, mint kukkolás (lásd Székely Iván írását kötetünkben) – ez az életük része.

Elgondolkodtam, mi mást csinálhatnának a tanulók otthon a számítógépen, mennyire ismerik az internet adta többi lehetőséget.

Kolléganőmmel, Juhász Erzsébet gimnáziumi tanárral, aki a történelem és a magyar mellett a társadalomismeretet is tanítja iskolánk diákjainak, egy különleges „projekthét” keretében lehetőségünk nyílt az egyik végzős osztállyal az információs társadalomnak szentelni kétszer három órát. Projektünk lényege az volt, hogy megismertessük a diákokkal a globális információs társadalom kialakulását, jelenkori jelentőségét. Célunk volt, hogy tisztában legyenek az interneten fellelhető információk hitelességével. Eszükbe jusson keresés és olvasás közben, vajon igaz-e, amit olvasnak. Nézzenek utána, kitől származik a hír, mikor került fel az internetre.

Megkérdeztük a jelen lévő harmincöt nagykorú diákot, hogy hányan vásároltak már az interneten (két fő), hányan „jártak” már elektronikus könyvtárban (négy fő, mind a négyen találkoztak ezzel nálam informatika fakultáción). Az internet veszélyeiről szóló kérdésekre is általában ugyanaz a három tanuló tudott válaszolgatni.

A második órára bevittünk egy feladatsort, amelyben az interneten elérhető különböző lehetőségeket szerettük volna felvillantani a gyerekek előtt. A diákok láthatóan még nem vettek igénybe hasonló szolgáltatásokat, de ezek megtalálása és megismerése nem okozott nekik gondot. Az osztály nagy részének figyelmét sikerült felkelteni a számukra új lehetőségek iránt. Kaptak egy beadandó házi feladatot is, amelyben a továbbtanulá-

sukkal kapcsolatos információkra kellett rákeresniük, és több kérdésre válaszokat kellett keresni a neten. Kolléganóm beszámolója szerint a gyerekek igen lelkiismeretesen végezték el ezt a feladatot.

Említettem, hogy a kerettanterv szerint a gimnáziumi négy évből összesen heti két informatikaóra jut kilencedikben. Egyre több iskolában nő ez az óraszám, de sok helyen csak a fakultáció ad lehetőséget a nagyobb óraszámra – a 11. évfolyamtól. Kivétel ez alól az úgynevezett nyelvi előkészítő szak, ahol a diákok nulladik évfolyamon, a tizenegy-tizenkét órás nyelvtanulás mellett heti négy órában tanulhatják az informatikát. Egy ilyen csoporttal volt lehetőségem részletesebben venni az internethez tartozó ismereteket. Ezt szeretném most megmutatni, idézve a gyerekek munkáiból.

Jelenleg nyelvi előkészítő, elsős (kilencedikes), tizenhét fős csoportomban szinte mindenki egy óránál többet ül naponta a gép előtt. Megkérdeztem őket is, hogy mivel töltik ezt az időt. Tíz-en az ismerősök keresésére készült portálokon nézegetik ismerőseikről a különböző híreket, illetve itt lévő alkalmazásokkal játszanak. Ketten tagjai valamilyen fórumnak, illetve ketten szoktak rendszeresen híreket olvasni az interneten. Talán a köztük lévő három év az oka, vagy csak a két társaság összetétele más, de ez a kilencedikes csoport jóval gyakorlottabban állt az internet témájához, mint a végzősök. A heti négy óra lehetőséget adott arra, hogy a végzősökkel végigvett projektet megismertessem velük. Az internet lehetőségeivel kapcsolatban például három-négy fős csoportokra bontottam a társaságot, és minden csoport kapott egy adott témakör köré felépített kérdéssort. Mindegyik témakör valamely internetes szolgáltatással állt kapcsolatban. Minden csoportnak volt húsz perce, hogy keressen a feladathoz tartozó webhelyeket, és válaszoljon a kérdésekre. Az idő leteltével be kellett egymásnak mutatniuk egyet-egyet az internet adta lehetőségek közül projektoron, kíséző magyarázattal. A csoport egyik tagja teljes tájékozottsággal beszélt az interneten való fizetés lehetőségeiről, és részletesen be is mutatott egy olyan oldalt, amely erre való. Összességében mégis azt éreztem, hogy sikerült

újdonságokkal is megismertetnem őket. Megbeszéltük, hogyan lehet vonatjegyet venni, pizzát rendelni, autópálya-matricára szert tenni, vagy külföldi vendégeinknek megadott időpontra színház- vagy koncertjegyet rendelni. Ezután az interneten előforduló veszélyeket is érintettük. Mivel a csoport haladó szinten tanulja az angolt, mindenkinek le kellett fordítania egy cikket egy olyan weblapról, amelyen úgynevezett hoaxok olvashatók, olyan hírek, amelyek az interneten valósként jelentek meg, de nem voltak igazak. (Az oldalt egyébként a könyv ötletét adó konferencián³ ismertem meg). Íme egy fordítás:

„Hallottam egy hírt tegnap a CNN-en. A hír szerint: Tupac Shakur életben van. Nem tudom elhinni, ő a kedvenc rapperem. Mindenki azt mondta, hogy vezetés közben lelőtték, amibe belehalt, de ez a cikk mindent megváltoztatott. A hírt a CNN weboldalán olvastam (gondoltam, ott megbízhatóak az információk). A cikk így hangzott: Tupac tegnap délután feltűnt Beverly Hillsben, egy bevásárlóközpontban, miközben vásárolt.

Másnap a csúf igazság feltűnik...

Oh, milyen szörnyű dolog ez! A cikk hamis volt. Valaki csinált egy weblapot, amely úgy nézett ki, mint a CNN oldala, ráadásul a webcím is nagyon hasonló volt. Nagyon, nagyon csalódott vagyok. Azt hittem, hogy még el tudok menni egy Tupac-koncertre ebben az életben. Mostantól nem fogok hinni ilyen weblapoknak, mint ez. De ha jobban belegondolok, még mindig el tudok menni egy 50 Cent-koncertre! Valójában Tupac jobb, mint 50 Cent, bocsánat, jobb volt.”

Másik kapcsolódó feladatuk az volt, hogy a chatelés nyelvén írjanak le egy történetet vagy párbeszédet. A legtöbben ezt viccesnek tartották, de amikor az órán párat kivetítettünk projektoron, és „le kellett fordítaniuk” egymás írásait, akkor többen megdöb-bentek az „új” nyelven. Ők, velem együtt, elég keveset értettek ebből a szlengből, de persze volt a csoportban egy-két profi fordító. Íme néhány idézet:

talmazó hírek és a szleng nyelvű párbeszéd mellett fel kellett tennünk legalább két dolgot, amit veszélyesnek tartanak az internettel kapcsolatban. Íme három idézet:

„Személyes adatok: amikor közösségi oldalakra regisztrálunk, rengeteg személyes adatot kérdeznek meg tőlünk, amikre nem kell feltétlen válaszolni, de ha muszáj, akkor ellenőrizni kell, hogy ezek az adatok sehol nem lesznek láthatóak.

Internetes vásárlás: Vigyázni kell, hogyha az interneten szeretnénk vásárolni, ne adjunk meg bankszámlaszámot, főleg ne olyan oldalon, ami kétes, mert több pénzt szedhetnek le a kártyáról, mint amennyit kéne.

Vírusok: sajnos több olyan internetes oldal van, amit ha megnyitunk, esetleg vírus kerülhet a gépre, főleg a letöltéseknél adódhatnak ilyen problémák.”

„Internetes vásárlás:

ha kártyával fizetünk semmiképp se adjuk meg a kártyánk kódját

- megeshet, hogy az áru nem úgy néz ki, mint a képen
- nem jó a méret, esetleg a minőség
- megeshet, hogy nem érkezik meg a rendelés”

„Chatelés:

Vadidegen embereknek ne add meg a telefonszámod, lakáscímed.

Ne küldj képet magadról, ha azzal visszaélhet.

Olyannak, akit nem ismersz, ne adj ki semmilyen fontos személyes információt.”

Kértem, hogy írjanak pár szót „Én és az internet” címmel is, ebből is idézek néhány gondolatot:

„Én egy átlagos internet használónak tartom magam. Napi 1-2 órát szoktam szörfölni a neten, ami alatt sok mindent megcsinálok. Például chatelek a barátaimmal, illetve megnézem a leveleimet, hátha jött valami fontos, hiszen manapság a levelezőfióko-

mat többször használom, mint a postaládánkat. Ennek tényleg vannak előnyei és hátrányai. Előny, hogy akármikor akárkivel tudom egyszerűbben és gyorsabban tartani a kapcsolatot, és olcsóbban és egyszerűen jutok a leveleimhez. Viszont szerintem semminek se szabadna felváltania a szemtől szembe beszédet. A fizikai kontaktus egy másik emberrel nem felcserélhető az internetes kapcsolattartással. Nagyon sok félreértés is adódik az ilyen beszélgetésből, mivel sok minden nem úgy megy át, mint ahogy azt szeretted volna. Elengedhetetlen lenne egy beszélgetésben a hangsúly, hangnem és így tovább. Nekem ez a véleményem az internetről.”

„Én az internetet főleg chatezésre használom. Szoktam ezenkívül ételt rendelni, tv-műsort nézni, és szavakat fordítani. Zenét nagyon szeretek hallgatni és videókat nézni. Nagyon jó, hogy mindenről lehet olvasni, és lehetőség van arra is, hogy kérdezzek szakértőktől, ha olyan dologról van szó. Tudok naplót írni, és ezt a lehetőséget is kihasználom. Ennek az az előnye, hogy ha akarom, csak én tudom a címét, és ha valaki rá is jönne, jelszót kérhetek, hogy elolvashassa. Ha a házi feladatomban nem tudok valamit, arra is egyszerűen választ találhatok. Ha van egy kedvenc zenekarom, vagy sorozatom, vagy bármim amiért rajongok és szeretném, hogy mások is megismerjék, készítek egy honlapot. Fontos még, hogy fel tudok regisztrálni közösségi honlapokra, és megismerni embereket akár más országból is.”

„Manapság már az internet szinte elengedhetetlen része a mindennapi életünknek. A tanárok van, hogy interneten adnak fel házi feladatot, az interneten lehet megnézni a hiányzó tanárokat. Valahol én igazságtalannak tartom, hogy ez egy elvárás, hogy legyen számítógépünk internet előfizetéssel. Nem szoktam sokat internetezni, szerencsére nem vagyok »gépfüggő«, és az online beszélgetések helyett én inkább a szemtől szembeni beszélgetéseket szeretem. Azt is gondolom, hogy rengeteg agresszív játék van, ami miatt az emberek is agresszívebbek lesznek, persze a szá-

mítógép eredetileg katonai célokból lett kifejlesztve. Mondhatok sok rossz tulajdonságot az internetről, de én is használom, mert nagyon hasznos is!”

„Néha nem vagyok róla meggyőződve, hogy az internet egy jó dolog. Persze, megkönnyíti a dolgunkat, de ez lustává teszi az embert. Nekem már sok ez a folyamatos kommunikáció. Nem értem, miért lett olyan fontos hirtelen minden második percben megírni, hogy éppen mit csinálsz. Én őszintén szólva jól megvagyok ennyi információ nélkül is. Emellett eltávolítja egymástól az embereket, hogy szinte csak a gépen keresztül beszélnek egymással. A személyes kapcsolat szerintem össze sem hasonlítható ezzel... Persze ez csak az árnyoldala a dolgoknak. Régen sokkal »nagyobb« tűnhetett a világ. Most már minden gond nélkül beszélhetsz bárkivel a Föld másik oldalán.

Mindenesetre szívesen kipróbálnám internet nélkül az életet. Viszonylag sokáig kibírta nélküle az emberiség, úgyhogy szerintem nélkülözhető. Kár, hogy ennyire központi dolog az életünkben a gépezés...”

„Elég sokat ülök a gép előtt és ez idő 80%-át internetezéssel töltöm. Szeretek a barátaimmal beszélgetni a chaten, és a különféle közösségi portálokon nézelődni. Elég sok zenét keresek az interneten és a videomegosztó oldalakon zenét hallgatok/keresgélek. Ha érdekel valami, azt beírom egy keresőbe. Szeretem a könyveket, ezért gyakran nézelődöm a könyvesboltok oldalain újdonságokat keresve. Előfordul, hogy ki akarok próbálni valamilyen új süteményt, és akkor könnyedén le tudok nézni egy-egy új receptet. Az internet szerintem jó dolog. Segítségével majdnem minden elérhető az ember számára. Közelebb hozza a külvilágot hozzánk. De mindeközben ügyelnünk kell a veszélyekre is, amik benne rejlenek.”

Az internet „hasznai”

Az internet nem csak az informatikaoktatásba hozott változásokat. Említettem, hogy az osztályok honlapokat készítenek maguknak. Közösségtől függ, hogy mennyire használják az elkészült lapokat, de ha jól működik a honlap, akkor az osztályt pillanatok alatt lehet értesíteni az esetleges változásokról, hírekről. Megnézve a különböző osztálylapokat, van, ahol chatszobák vannak, elérhető az órarend, házi feladatok, fényképek. Szinte mindegyiken megtalálhatóak a tanárok aranyköpései. Itt meg kell jegyeznem: nem hiszem, hogy a tanárokat megkérdézik, feltehetik-e a viccesnek ítélt mondatokat az internetre.

Az iskolák is igyekeznek minél több információt megosztani az interneten. Ha a szülő és gyermeke iskolát keres továbbtanulás céljából, az első ítéletet az iskola honlapja adja. Mit ír magáról az intézmény? Milyen képek, rendezvények, órák, tanárok láthatók, van-e esetleg vendégkönyv, ahol beszélgetni lehet a már ott tanulókkal? Az iskola nemcsak a felvételizőket, hanem saját tanulóit is tájékoztathatja a honlapon keresztül például az aktuális helyettesítésekről, versenyeredményekről, programokról.

Az internet a tanár-diák kapcsolaton is sokat változtatott. Sok tanár természetesnek tartja, hogy első órán felírja a táblára az e-mail címét, és írhatnak neki a diákok, ha kérdésük van. Nekem természetes, hogy az informatika órai beadandó feladatokat e-mailen küldik el a gyerekek. Szinte minden csoportomból van egy-két tanuló, akivel rendszeres levelezésbe kerülök, hol „távkorrepetálást”, hol személyes beszélgetéseket bonyolítunk. Ha a gyerekek nem értik a házi feladatot, MSN-en állandó kapcsolatban vannak, és akkor is meg tudják beszélni egymással a feladat megoldását, ha éppen a város két végén laknak.

Az internet nem csak az iskolán belüli, hanem az iskolák közötti kapcsolatokat is megkönnyíti. A mi iskolánk is kapcsolódott a Comenius programhoz. „A program célja, hogy az általános és középiskolás diákok, valamint tanáraik tudatára ébredjenek az európai kultúra sokszínűségének, és felismerjék annak

értékeit. Támogatja továbbá azon alapkészségek elsajátítását, amelyek a fiatalok személyes fejlődéséhez, jövőbeni munkába állásához és európai közéleti szerepvállalásához szükségesek.”

A program keretein belül iskolánk három külföldi iskolával vette fel a kapcsolatot. Tanulóink a partnerkapcsolat építése során állandó levelezőpartnerekre találtak; képeket, videókat, verseket, írásokat készítettek, fordítottak le és osztottak meg a többi iskolában tanulókkal, illetve mindenkivel, aki ellátogat a projekt leírását tartalmazó honlapra. Ennek a projektnek része volt az internet állandó használata, a weblapkészítéstől, a programokról készített beszámolón át az úgynevezett virtuális lábnyom készítéséig.

Összességében elmondható, hogy az informatika fejlődésével együtt változik a gyerekek viszonya az internethez, egyre jobban ismerik, egyre többet használják. Ebből adódóan talán a kockázatok és a veszélyeket is jobban fel tudják mérni, több ilyen témájú hír jut el hozzájuk. Ennek ellenére, vagy éppen ezért nagyon fontosnak tartom, hogy minél alaposabban tájékoztassuk a fiatalokat a felmerülő veszélyekről, s megismertessük velük azt a rengeteg lehetőséget, amelyet az internet tartogat számukra.

Vajda Zsuzsanna *Pszichológus, egyetemi tanár,
a kultúra és a felnevelkedés összefüggéseinek kutatója,
szakkönyvek, tanulmányok, népszerű könyvek szerzője*

A GYEREKEK ÉS A SZÁMÍTÓGÉP

Valahányszor a kisgyermekes médiahasználatáról tartok előadást, a hallgatóságból néhányan mindig megjegyzik, hogy óvodás korú gyerekük már önállóan használja a számítógépet: be tudja kapcsolni, és a böngészőn megtalálja az őt érdeklő dolgokat. Egy édesanya elmesélte, hogy férjével jelszavassá tették a számítógépbe való belépést, hogy óvodás gyerekük ne használhassa a tudtuk nélkül. Néhány hét után megdöbbenve vették észre, hogy a gyerek kileste, milyen billentyűket ütnek le a szülei, és be tudja kapcsolni a gépet. Saját unokám még nem volt hároméves, amikor meg tudta mutatni, melyik gombot kell megnyomni, ha ki akarjuk venni a laptopból a DVD-t.

A gyerekekre szinte születésüktől fogva nagy hatást gyakorol a képernyő, és használatát tekintve hallatlanul tanulékonyak – természetesen csak akkor, ha környezetük ezt lehetővé teszi. Ma már azonban a mi kultúrkörünkben, így Magyarországon is, a családok túlnyomó többsége rendelkezik számítógéppel. Nem

meglepő, hogy a gyerekek kedvelik: filmeket, képeket, meséket lehet nézni rajta, és feltehetően még ennél is erősebb motívum, hogy mi, felnőttek, intenzíven használjuk. Amikor hazaérünk, első dolgunk, hogy bekapcsoljuk a gépet, izgatottan olvassuk a híreket, leveleket. Márpedig a gyerekek, amióta világ a világ, mindig azt szerették volna tenni, amit a felnőttek.

Alig több mint két évtizeddel ezelőtt a szakemberek arra számítottak, hogy a számítógép elsősorban az elit és a középosztály „játéka” lesz. Ez azonban ugyanúgy tévedésnek bizonyult, mint a televízió és a mobiltelefon esetében. A személyi számítógépek megjelenését követően a széles körű felhasználási lehetőségekre reagálva váratlan gyorsasággal megjelent a tömegigény, amelynek nyomában létrejöttek az olcsó gyártási technológiák, és a számítógép és az internethasználat elképesztő sebességgel terjed az egész világon. A fejlett országokban a számítógép használata a mindennapok része, sőt nélkülözhetetlen tartozéka lett. A számítógép és az internet sokoldalú felhasználását a szórakozástól az ügyintézésig nem is érdemes sorolni, hiszen valamennyien ebben élünk. Bár a teljes lakosság körében az internethasználat a fejlett országok átlagát tekintve még viszonylag alacsony, a tanulók körében a lefedettség már Magyarországon is megközelíti a 80%-ot.

Az a tény, hogy a számítástechnika ilyen mértékben beépült az életünkbe, materiális és eszmei értelemben is elkerülhetlenné teszi a gyerekek bekapcsolódását. Az is természetes, hogy a szülők fontosnak tartják, hogy gyermekeik megfelelő készségekre tegyenek szert a számítógép kezelésében. Valójában azonban nagyon keveset tudunk arról, hogyan befolyásolja a fejlődést az a tény, hogy a digitális elektronika a mindennapi élet alkotórésze lett. Az önmagában is nagyon komplex kérdésnek több különleges aspektusa van a gyerekkorra nézve.

Az első probléma: az életkori határ kérdése. Nincsenek megbízható, és különösen nincsenek független vizsgálatok, sem tapasztalatok arra nézve, milyen hatást gyakorol az első években a gyerekekre a számítógép használata, van-e szükség életkori korlátra. Mint arra majd részletesen is kitérünk, a televízió nézésé-

vel kapcsolatban vannak kutatási eredmények, amelyek óvatosságra intenek.

A második probléma: ezzel az új kommunikációfajttával tovább folytatódik a trend, amelynek során bizonyos felnőttek, elsősorban a szülők és a pedagógusok, egyre inkább elveszítik kontrolljukat a gyerekek-fiatalok kultúrája, időtöltése fölött.

Igaz, nem minden kutató tartja egyértelmű hátránynak, hogy a gyerekek „egy kis magánéletre” tesznek szert a számítástechnika segítségével. Anonim környezetben felszabadultabban beszélnek olyan összetett problémákról, mint a szexualitás vagy a párkapcsolatok. Másrészt a számítógépen folytatott tevékenységükbe nem avatkoznak be a szülők, sem a testvéreik. Bizonyos fókig természetesen felfogás kérdése, hogy a kontroll nélküliség előnyt vagy hátrányt jelent-e. A szerzők is megállapítják, hogy a gyerekek gyakran játszanak, barátaikkal csevegnek otthon és az iskolában a számítógépen keresztül, miközben úgy tesznek, mintha tanulnának (lásd Talyigás Anikó és Z. Karvalics László fejezetét). Hangsúlyoznunk kell ugyanakkor, hogy csak bizonyos felnőttek kontrollja és befolyása csökken, a szülőké és a pedagógusoké, akik a gyerekek sajátos szempontjait képviselnék. A tömegkommunikációt ugyanis szintén felnőttek működtetik. Az anonimitás nyújtotta felszabadság is ellentmondásos, hiszen a látszólag privát környezet voltaképpen a legbizalmasabb személyes információk nyilvánosságra kerülését, vagy legalábbis annak kockázatát jelenti.

Írásomban arra teszek kísérletet, hogy összefoglaljak néhány fontosabb kutatási eredményt és véleményt, amely a média gyerekekre gyakorolt hatásával kapcsolatban ma hozzáférhető. Úgy tűnik, hogy érdemes különválasztani a számítógép-használatba való bekapcsolódás hatását a kisgyermek megismerő funkcióira, értelmi fejlődésére, és az elektronikus kommunikáció hatását az idősebb gyerekekre. Ez utóbbi jóval komplexebb problémakör, hiszen a „fogyasztott” tartalom csak egy része a problémának. Az iskoláskorú gyerekek közösségei, kapcsolatai, szórakozási és tanulási szokásai is egyre inkább a számítógép használatához kötődnek. Az ehhez kapcsolódó, szerteágazó problémakört, amely-

ről szintén nincs még megfelelő tudásunk, legfeljebb néhány elemében tudjuk érinteni egy ilyen tanulmányban. Írásom utolsó részében végül arra szeretnék kitérni, miért volna szükség a gyerekek védelmére, és miért vallanak folyamatosan kudarcot az erre irányuló kísérletek.

A kisgyermek és a számítógép

A kisgyermekes számítógép-használatáról, ahogyan már erről szó esett, kevés adattal rendelkezünk – jobban mondva rengeteg szolgáltató kínálja korai fejlesztőprogramjait, amelyek szenzációs eredményekkel kecsegtetnek. Valójában a televízió kisgyermekre gyakorolt hatását szemlélve kétségeink ébredhetnek a korai számítógép-használat előnyeivel kapcsolatban. A kutatási tapasztalatok azt mutatják, hogy a 2-3 éves gyerekek még egyáltalán nem tudnak különbséget tenni a televíziós kép és a valóság között. A kicsik megszólítják a képernyőn látott figurákat, integtetnek nekik, sőt egy kísérlet tanúsága szerint tartanak attól, hogy a képernyőn kiborított pattogatott kukorica kihullik a szoba szőnyegére. Egy másik kísérletben a kutatók azt találták, hogy óvodáskor előtt a gyerekek úgy gondolják: a tévében szereplők beléphetnének az ő szobájukba.

Körülbelül 4 éves koruktól a gyerekek már megértik, hogy amit a képernyőn látnak, az nem a valóság, hanem annak egy ábrázolása, ám meg vannak róla győződve, hogy ez az ábrázolás realisztikus. Még a 6-7 éves gyerekek is csak akkor veszik észre, hogy valami biztosan fikció, ha durván megsérti a valóság szabályait, például ha a kutya embertestű van, vagy ha az állatok beszélnek. Csakhogy miközben sok esetben tudják, hogy a látvány képtelenség, gyakran félelmetesnek találják az ilyen figurákat. Strasburger és kutatótársai egy 2009-ben megjelent tanulmányban arról számolnak be, hogy kutatási tapasztalataik szerint még az 5 éves gyerekek is biztosak voltak benne, hogy a Cukros Boszorkány nevű mesefilmfigura valóban létezik, és elhitték, hogy

cukrot tud hagyni a lakásban. Magát a kategóriát, hogy valami lehetséges vagy sem, csak iskoláskorban kezdik használni a gyerekek. Az óvodás gyermekek a tartalomnál sokkal inkább figyelnek a hangokra, vizuális effektusokra. Percepciójuk a tartalom értelmezésénél is alapvetően befolyásolja őket: így például kísérletek tanúsága szerint hajlamosak úgy ítélni, hogy a csúnya, rossz külsejű szereplők gonoszak is, miközben néhány évvel idősebb társaik már képesek a distinkcióra.

Az extenzív és irányítatlan televíziózással kapcsolatban hangzottatott bírálatok között az is szerepelt, hogy a gyerekek valóságképe a látottaknak megfelelően alakul. Több anekdota szerint a sokat tévéző mai óvodások azt hiszik: a halál oka mindig az, hogy agyonlövik az embert, és úgy beszélnek a dinoszauruszokról, mintha a szomszédjukban laknának.

Okkal feltételezhető, hogy a valóságészlelés szempontjából a számítógép-használat még kritikusabb, mivel a számítógép interaktív, ezért komplexebben és differenciáltabban hat a felhasználó megismerési folyamataira, mint a televízió.

A rendelkezésre álló szórványos tapasztalatok alapján is aggodalomra ad okot, hogy a korai számítógép-használat bonyodalmakat idézhet elő a gyermek saját érzékszerveinek használatában, mozgásvezérlésében. A digitális kommunikáció a valóság különleges része: olyan valóságelem, amelynek megfejtése nem lehetséges az egyszerű tapasztalás eszközeivel. A tárgyi valóság elemeit a gyerekek saját érzékszervei, látása, hallása, tapintása közvetítik. A számítógépen keresztül azonban a valóság szignifikáns elemei torzítva, gépi közvetítéssel érkeznek el a gyerekekhez, áttétel iktatódik a saját érzékelésük-észlelésük és a valóság közé. Ehhez a kódrendszerhez nincsen természetes dekódoló apparátusuk.

Egy példa: azt, hogy a távolabb lévő tárgyak valójában nem kisebbek, mint a közelebbiek, maguktól megtanulják a gyerekek, mivel az ezzel kapcsolatos sokezernyi élmény egyforma. Ám abban, hogy miért tűnnek el bizonyos emberek, tárgyak a képernyőről, a kisgyermek számára nincs következetesség, nem igazít

el a spontán tapasztalat. Ezáltal zavar keletkezhet a kisgyermek-kori fejlődés egyik legfontosabb folyamatában, a kisgyermek gondolkodásmódjára ugyanis éppen az a jellemző, hogy nincs egyértelmű határvonal a fikció és a valóság között. A mágikus gyermeki világtépből fokozatosan alakul ki a fejlődés és érés folyamán a valóság összefüggéseinek racionális, felnőtt interpretációja.

A fejlődés fent vázolt jellegzetességei és a televíziózás kapcsán összegyűlt tapasztalat fényében tehát nem megnagyító, hogy a kisgyermek egyre korábban ismerkedik meg a számítástechnikával. Egy 2000-ben készült felmérés eredményei azt mutatták, hogy az Egyesült Államokban a 2–5 éves gyerekek 27%-a volt kapcsolatban naponta legalább fél órán át számítógéppel. Márpedig az igazi áttörés, a tömeges használat az elmúlt tíz évben vált valósággá a fejlett országokban. Wartella és Jennings kutatásai arra is felhívják a figyelmet, hogy a számítógép nem közösségi médiaeszköz. Ez a lakáson belüli elhelyezkedésében is tükröződik: amíg a televízió, különösen az első évtizedekben, a közösségi helyiségekben volt, a számítógép személyes holmi, a családtagoknak saját számítógépük van. Ez a tény igencsak megnehezíti a szülői kontrollt és közreműködést. A saját számítógéppel való rendelkezés is terjed a gyerekek körében, egy 2005–2006-ban készült amerikai felvétel adatai szerint a 4–6 éves korú gyerekek 7%-ának már saját számítógépe volt. Iskolakezdekor az arány hirtelen megnőtt, a 8–10 évesek körében már 23%. Minden okunk megvan rá, hogy feltételezzük: mára ezek az arányszámok még nagyobbak, és a rendelkezésre álló adatok alapján nagy valószínűséggel állítható, hogy a helyzet Magyarországon sem tér el ettől jelentősen. Török Balázs 2001 és 2003 között gyűjtött adatai szerint a mintát alkotó több mint négyezer óvoda családjainak 60%-a rendelkezett számítógéppel. Újabb adatok a gyerekek számítógép-használatáról nincsenek, de az általános lefedettség és használat nem tér el a fejlett országokétól.

Kisgyerek – számítógép – üzlet

Bár – mint a bevezetőben is szó esett róla – a gyerekek spontán is érdeklődnek a kommunikációs eszközök iránt, ez csak részben oka a korai használtnak. Az elmúlt években a televíziós csatornák versengve készítettek egészen kicsi gyerekeknek szóló műsorokat, majd tömegével dobták piacra az immár számítógéppel lejátszható „fejlesztő DVD-keket”, amelyek azt ígérik a szülőknek, hogy segítségével a gyerekek értelmesebbek lesznek, hogy használatuk elősegíti a matematikai készségek fejlődését, a szókincs bővülését, sőt szociálisabbá válnak! Kyrkorian és munkatársai tanulmányukban 2008-ban ezért fontosnak tartják leszögezni, hogy a másfél évnél fiatalabb gyerekek még egyáltalán nem értik, mi történik a képernyőn. A beszélni még nem tudó kisgyermek médianézését úgy vizsgálták, hogy a szemmozgásukat vették videóra. A kísérlet folyamán a Teletubbies egyik epizódját mutatták a gyerekeknek, de az epizódot elrontották úgy, hogy összekeverték a jelenetek részleteit. A gyerekeknek szemmozgásuk alapján másfél éves koruk előtt egyáltalán nem tűnt fel a változás. Teljeséggel légből kapott tehát az az állítás, hogy a csecsemők és kisdetek bármit is tanulnának a képernyőn látottakból. Hasonló kutatási eredmények alapján a Walt Disney cég a közelmúltban kénytelen volt felajánlani, hogy megteríti a *Baby Einstein* című, általa forgalmazott videó árát.

A kutatási eredmények alapján az ezt követő másfél-két évben is elsősorban saját tapasztalataikból tanulnak a gyerekek, sőt azt is megállapították, hogy azoknál, akik kicsi koruktól sok időt töltöttek a képernyő előtt, kialakult egy sajátos szindróma, a „videodeficit”. A kisgyerekek alkalmanként utánozzák a képernyőn látottakat, de ezek jelentése egyáltalán nem nyilvánvaló a számukra. Képesek szavakat is tanulni a televízióból vagy a számítógépről, de a saját és az idegen nyelvi fonémák megkülönböztetése kevésbé sikeres az így tanult szavak alapján. A problémakör természetesen még nincs alaposan feltárva, de a kockázatok világosak. Az Amerikai Gyermekgyógyászok Szövetsége (American Academy of Pediatrics) többször is nyilvánosságra hozta ál-

lásfoglalását, amely szerint a 2 évnél fiatalabb gyerekek számára mindenféle televízió- és videonézés ellenjavallt. Mindennek ellenére folyamatosan kerülnek forgalomba a kisgyermekeknek szóló, többnyire didaktikus célt hordozó videók és számítógépes programok. A gyerekek képernyőhöz szoktatását igen határozott anyagi-financiális szempontok támogatják. A gyerekek köztudomásúan igen lelkes nézőcsoportot jelentenek, és igen jelentős az a nyomás, amelyet különböző cikkek vásárlása érdekében kifejtenek. Kisgyermekkel foglalkozók tudják, hogy a képernyőn látottak megjelennek a gyerekek játékaiban, asszociációiban.

Az óvodások esetében már a tartalom befolyásával is számolni kell. Felnevelkedésük során a mai gyerekek a hirdetések elképzelhetetlen tömegével találkoznak. 2002–2003-ban a 4–12 évesek javaslatára a szülők harmincmilliárd dollárt költöttek különféle fogyasztási cikkekre és szolgáltatásokra, a 17 éven felüliek pedig százmilliárdnál is többet. Emellett nem tűnik kimondottan nagynak az egyébként szintén jelentős, tizenöt milliárdos összeg, amelyet a cégek marketingre költenek.

Bár továbbra is a televízió marad a fő támadáspont, az új médiafajták is előtérbe kerülnek, új hirdetési stratégiával. Az internetes marketing több okból is lényegesen veszélyesebb, mint a televíziós. Az interneten könnyebb közreadni a burkolt, rejtett hirdetéseket, másrészt a szabályozásra szinte egyáltalán nincs lehetőség, hiszen az internetet a hirdetések tartják el. A kutatási eredmények viszont egyöntetűen azt mutatják, hogy a 8–9 éven aluli gyerekek esetében a médiahatás jóval közvetlenebb, mint a felnőtteknél, például meghatározott ételhirdetések hatására a gyerekek valóban többet ettek.

Kockázat vagy nyereség?

Attevel és munkatársainak 2008-as megállapítása szerint a szülőknek szóló útmutatók többségében az olvasható, hogy a gyerekek 3–4 éves koruk körül már érettekké válnak a számítógép hasz-

nálatára. Valójában mindössze arról van szó, hogy ilyenkor már képesek önállóan bekapcsolni a gépet, és próbálkoznak az egér használatával is. A kockázatok tekintetében megoszlanak a vélemények. Seymour Papert,¹ az elektronika egyik úttörője, a gyerekek számítógép-használatának nagy propagálója egy különleges programozási nyelvet is kifejlesztett a gyerekek számára (LOGO). Véleménye szerint a számítógép-használat nagyon kedvező hatással van a gyerekek értelmi működésére, általa megérthetik, hogyan működnek saját kognitív funkcióik. A 2000-es években számos országban kormányprogramok segítették elő az óvodás korú gyermekek számítógép-használatát – természetesen a gyártók hathatós nyomásának engedelmeskedve. Magyarországon ez a kampány a „kakaóbiztos számítógép ügye” néven vált híressé.² (Lásd Z. Karvalics László írását kötetünkben.)

Ugyanakkor nem kevesen vannak, akik a potenciális veszélyekre hívják fel a figyelmet: az Alliance for Childhood nevű amerikai civil szervezet egyenesen moratóriumot szeretett volna bevezetni a gyerekek számítógép-használata ellen. A közelmúltban több internetes portálon olvasható volt, hogy egy angol pszichológus, dr. Aric Sigman szerint a számítógép korai használata hátrányosan befolyásolja a kisgyermekek kognitív fejlődését.³ Sajnos, ahogyan ez az utóbbi időben egyre inkább szokássá válik, a cikkekben nem hivatkoznak az ezt alátámasztó kutatásra. A kockázatok valójában itt is feltáratlanok, vagy nem kapnak nyilvánosságot. Schmidt és munkatársai némi csodálkozással állapítják meg, hogy a gyerekek számítógép-használatára vonatkozó kutatási eredmények egyáltalán nem befolyásolták a politikai döntéshozatalt. Pedig a számítógépet rendszeresen használó óvodások esetében a negatív hatások között szerepel a látáskárosodás, valamint többszörös megerősítést nyert, hogy összefüggés van a túlsúlyosság és a médiafogyasztás között. Egyre többen vannak az óvodások közül, akik felfedezik a számítógépes rajzolás lehetőségét, és olyanok is, akik ennek következtében nem rajzolnak ceruzával. A kézizomzat finommotoros koordinációjának leszűkülése az egérmozgatásra azzal a kockázattal jár, hogy problémák

mutatkoznak a későbbi ceruzafogásban, valamint a fogás, a manipuláció más helyzeteiben is.

A kisiskolás korú gyerek és a számítógép

Az iskolába lépés az a határ, amikor a gyerekek mindenképpen megismerkednek a számítógéppel. Erre az időszakra a korábbi kockázatok csökkenni, bár a fikció és a valóság megkülönböztetése, különösen a kereskedelmi célú üzenetek felismerése, csak 8–9 éves korban válik biztonságossá. Ma már a számítógép és az internet használata iskolai tananyag (lásd Talyigás Anikó írását kötetünkben), az azonban kérdés, hogy helyes-e rögtön az első osztályban, az írás- és olvasástanulás előtt elkezdni. A legtöbb pedagógus megnyugtatóbbnak látja, ha a gyerekek csak azután válnak rendszeres számítógép-használóvá, miután megfelelő olvasási és íráskészségre tettek szert. Sajnos a számítástechnikai ipar hallatlan anyagi forrásai segítségével jóval hatékonyabban tudja befolyásolni a döntéshozatalt, mint a pedagógus és gyermekpszichológus szakemberek. Ennek köszönhető, hogy több országban irreálisan korán elvárják a gyerekektől a számítástechnika ismeretét. A Microsoft a közelmúltban kezdeményezte, hogy a gyerekek iskolai teljesítményének tesztelésénél is térjenek át a számítógépre, beleértve az alsó tagozatot is. Holott a tartalmi hatások szempontjából a kisiskolás, 7–12 éves korosztály a legveszélyeztetettebb, mivel egyre jobban tudja használni a gépet és az internetet technikailag, ugyanakkor élettapasztalata és valóságismerete még nem elégséges hozzá, hogy megóvja a potenciális veszélyektől. A kaliforniai egyetem, az UCLA kutatója, P. Greenfeld gyerekek chat-szobáinak tanulmányozása során elszörnyedve tapasztalta a durva hangnemet, az obszcenitást és a rasszizmus tobzódását. Azt tanácsolja a szülőknek, hogy csak moderált chathasználatot engedélyezzenek gyermekeiknek, vagy igyekezzenek ellenőrizni a használatot. Ez az életkor, amikor a leginkább megközelíthetők a gyerekek a pedofilok vagy a naivságukkal visszaélők számára. Betörések is tör-

téntek, miután a rablók a gyerekek internetes társalgásából megtudták, hogy egyedül vannak otthon.

Bár nem kétséges, hogy a számítógép és az internet használata rendkívüli mértékben bővítette az oktatás lehetőségeit, kutatási eredmények azt mutatják, hogy az iskolák és a pedagógusok csak korlátozottan képesek kihasználni a számítástechnika lehetőségeit. Schmidt és munkatársai 2008-ban tanulmányukban arról írtak, hogy a pedagógusok siettek beépíteni az internetes technikát saját tevékenységükbe, többek között az olvasástanításba is. A hatékonyságról ugyanakkor nagyon kevés adattal rendelkezünk. A közelmúltban végzett kutatások eredményei szerint nem hatékonyabb az internetes tanulás, mint a hagyományos, és az is bebizonyosodott, hogy a tanárok elsősorban saját kényelmük érdekében használják, azon a szinten, amennyire ők értenek hozzá. Nem látszik beigazolódni az a feltételezés, hogy a technika mindenképpen okosabbá teszi a gyerekeket.

Internet és tanulás, valamint az információtorzulás

A hazai szaksajtóban is helyet kapott az a vita, amely a számítógép- és internethasználat, valamint a tanulás kapcsolatáról szólt. Hammer Ferenc esettanulmányában beszámol róla, hogyan torzulnak többek között a gyerekek számítógép-használatával kapcsolatos információk. Az OECD 2000-ben készült PISA felmérése pozitív összefüggést talált a gyerekek tanulmányi eredménye és számítógép-használat között. Az eredményeket egy német szerzőpár megkérdőjelezte. Azzal érveltek, hogy nem oksági jellegű összefüggésről van szó: mind a tanulási teljesítményt, mind az internethasználatot a családi háttér befolyásolja döntő mértékben. Megállapításuk szerint, ha a családi háttér faktorát figyelmen kívül hagyjuk a kutatásban, akkor az internethasználat és az iskolai teljesítmény között egyenesen negatív összefüggés áll fenn. Ugyanakkor kiemelik, hogy ez sem oksági természetű, valamint felhívják a figyelmet az iskolai teljesítmény összetett,

soktényező háttérére. A német szerzőpár tanulmányának következménye Hammer kifejezésével élve „prérítűz” volt, amely a BBC-től indult ki: a kutatók mondanivalóját jócskán leegyszerűsítve azt közvetítette a közönségnek, hogy azok a gyerekek, akik sokat ülnek a számítógép előtt, rosszabb tanulók, mint azok, akik keveset. A híradás nyomában interpretációk egész sorozata keletkezett, valamennyi azt emelte ki, hogy a számítógép-használat a tanulmányi eredmény romlásához vezet. A negatív hatást egyre súlyosabbnak értékelték az egymás után megszólaló médiuumok. A kampány a hagyományos eszközökből – rádió, nyomtatott sajtó – indult ki, de a net-nyilvánosság – állapította meg a szerző – nem volt képes ellensúlyt alkotni.

Attevel és munkatársai arra hívják fel a figyelmet, hogy az internethasználat tanulásra gyakorolt hatásának vizsgálatánál gyakran az iskolai internethasználat mennyiségét vetették össze az iskolai teljesítménnyel. Ez azonban félrevezető, az iskolai számítógép-használat időtartama nem jó paraméter. A kedvezőtlen szociális helyzetű gyerekek, akiknek nem volt otthon számítógépük, többet használták a gépet az iskolában, de nem a tanulással összefüggésben. Más esetekben is fény derült rá, hogy a gépeket valójában nem az órákon használják, főként technikai problémák miatt. A szerzők empirikus vizsgálatot is készítettek, összesen 1680, 4 és 13 év közötti gyerek számítógép-használatát mérték fel a szülők és a gyerekek által közösen készített naplók segítségével. A kutatás eredményei arra hívták fel a figyelmet, hogy a gyerekek otthoni számítógép- és internethasználata csak minimális mértékben kapcsolódik a tanuláshoz. Azok a gyerekek, akiknek volt otthoni számítógépük, csaknem annyi időt töltöttek a gép mellett, mint a felnőttek. A mérsékelt használók esetében (kevesebb mint nyolc óra egy héten) találtak némi pozitív összefüggést a tanulási teljesítménnyel, de ez minimális volt. A fokozott használók esetében a legfontosabb összefüggés az volt, hogy ők jóval kevesebbet tartózkodtak a szabad levegőn. Egyéb tulajdonságaikban nem mutatkozott különbség, kivéve a testtömegindexet, amely határozottan nagyobb volt, mint a nem használóké.

A gyerekek és a médiahasználat

Egy amerikai szerzőpár, Roberts és Foehr közelmúltban keletkezett írásukban igyekeznek teljes keresztmetszetében feltérképezni, hogyan használják a gyerekek és fiatalok a médiát, amely – a szerzők kifejezése szerint – előnti őket. A tipikus 8–18 éves amerikai gyerek lakóhelyén három televízió van, ezenkívül szinte valamennyien rendelkeznek mobiltelefonnal és mp3 lejátszóval vagy iPoddal. Emellett használják a számítógépet is. A használat pontos ideje nehezen megítélhető, ugyanis a gyerekek gyakran televíziót néznek mosogatás közben, és időnként rápillantanak a számítógép képernyőjére is. Megjegyzendő, hogy a világon mindenütt folyamatosan nő az utcán vagy a járműveken fülhallgatóval közlekedő fiatalok száma, és egyre többen interneteznek a mobiltelefonjuk segítségével, vagyis folyamatosan „be vannak kapcsolva”, miközben a fizikai valóság elhalványodik a számukra.

Roberts és Foehr idézett kutatása szerint 2005-ben már a 6 éven aluliak naponta két órát töltöttek médiahasználattal. A 2–7 évesek három és fél órát voltak média jelenlétében, náluk az aktív használat ideje csaknem három óra volt. A 8–18 éveseknél a médiával töltött idő hét és fél órára növekedett, az aktív médiahasználat öt óra negyvennyolc perc volt naponta. Ez csak úgy lehetséges, hogy az adott korosztály több eszközt is használt egy időben. Míg összességében a médiahasználat időtartama nőtt az évek folyamán, az aktív médiahasználat nem. Az utóbbi valószínűleg már korábban elérte a plafont, viszont tovább nő a médiahasználat összesített ideje és a használt médiaeszközök száma. A médiával töltött időnek körülbelül a fele filmnézés volt a 8–18 évesek körében, s ez az arány alig változott ahhoz képest, amikor még a televízió volt a legfőbb médium. Ugyanakkor folyamatosan nő a videojátékokkal és számítógépes játékokkal töltött idő. Valójában tehát a televíziónézés alig csökkent, hiszen a gyerekek és fiatalok párhuzamosan más eszközöket is használnak.

Roberts és Foehr más kutatások eredményeivel egybehangzóan azt találták, hogy nagymértékben eltért a szülők és a gyere-

kek képe a gyerekek médiahasználatával kapcsolatban. A szülők igyekeznek elhíttetni magukkal, hogy a gyerekek jóval kevesebbet ülnek a számítógép előtt, mint amiről maguk a gyerekek beszámolnak. Eközben széles körű tapasztalat, hogy az újonnan beszerzett kommunikációs eszközök folyamatosan a gyerekek szobáiba vándorolnak, ami ugyanakkor azt is világosan mutatja: a szülőknek nemigen nyílik módjuk rá, hogy megtudják, hogyan használják gyermekeik a médiát. Az adatok azt is jelzik, hogy azok a gyerekek, akiknek a szobájukban volt a televízió vagy a számítógép, több időt töltöttek vele, mint azok, akiknél a kommunikációs eszközök máshol találhatók.

A fejlett országokban ma már minimálisra csökkent azoknak a száma, akik egyáltalán nem férnek hozzá a számítástechnikai eszközökhöz, de a digitális szakadék nem szűnt meg – állapítja meg Roberts és Foehr. Az alacsonyabb jövedelmű családban nevelkedő gyermekeknek az Egyesült Államokban is jóval ritkábban van otthoni számítógépük. Az egyetemet végzett szülők 17 éven aluli gyerekeinek több mint 90%-a, a középiskolát végzetteknek viszont csak 80%-a rendelkezett vele. Az egyes etnikai csoportok körében is jellegzetes eltérésekkel találkozottak a kutatók a médiahasználat tekintetében: a fekete családok gyermekei kezdettől fogva több időt töltöttek a képernyők előtt, mint a spanyol családokéi, és jóval többet, mint a fehérekéi. Ez az adat egybevág a hazai szakértők megállapításaival, amelyek szerint a magasabb iskolázottságú szülők inkább kontrollálják gyermekeik számítógép-használatát, mint a kevésbé iskolázottak. A fekete családok gyermekei nagy affinitást mutattak a tematikus műsorok, a filmek és sorozatok iránt. A különbségek később is fennmaradtak, sőt tovább nőttek: a fekete gyerekek és fiatalok napi nyolc-tízórás médiafogyasztásról számoltak be, ami azért is figyelemre méltó, mert a pusztán audioeszközök kevésbé voltak népszerűek körükben. Egy 2004-es kutatás azonban ettől némileg eltérő eredményre jutott: eszerint a médiahasználat nemcsak az alacsony, hanem a magas jövedelműek körében is nagy, mintegy U alakú görbét ír le.

Roberts és Foehr megállapítása szerint az Egyesült Államokban az iskolák „behálózottsága” szinte teljesnek volt mondható. Azokban az iskolákban, ahol a szegénység nagy koncentrációjú volt, jóval több tanuló osztozott az iskolai számítógépeken. Az ilyen környékeken működő iskoláknak ritkábban volt saját honlapjuk, ahol a közösség tagjai kommunikálhattak egymással.

Nagy különbséget tapasztaltak a tekintetben is, hogyan használják a gyerekek a gépet: a nagyobb jövedelemű családok gyermekeinek 77%-a használt számítógépet házi feladata megoldásához, míg a szegényebbeknek csak 29%-a. A digitális szakadék tehát megmaradt, csak kevésbé bináris jellegű, inkább fokozatos – állapítják meg a szerzők. A jó és a rossz tanulók médiafogyasztása között nem találtak jelentős különbséget, ugyanakkor megerősítve látják azt a mások által is regisztrált tényt, hogy a frusztrált, elégedetlen fiatalok robusztusabb médiafogyasztók, mint a kiegyensúlyozottak.

Hazai adatunk sajnos egyáltalán nincs arra nézve, mekkora a hátrányos helyzetű roma lakosság hozzáférése az internethez, holt ez a körülmény ma már az egész életutat megszabhatja – például a vállalkozók csak elektronikusan vallhatják be az adójukat! Harmadik világbeli tapasztalatok szerint mélyülő szakadékok idézhet elő a számítástechnikai kultúrából teljes mértékben kívül maradt szülők és gyermekeik között e kulturális eltérés. Az ilyen helyzetbe került szülők természetesen semmiféle útmutatást nem tudnak adni a számítógép és az internet használatával kapcsolatban, így a gyerekek fokozottan ki vannak téve a gyakran destruktív, ellenőrizetlen kortársi hatásnak.

Mint az elektronika minden vívmánya, a számítógép- és internethasználat is a serdülők körében a legnépszerűbb. A fiatalok a média legaktívabb használói is. Értékelik, hogy a korszerű médiaeszközök lehetővé teszik az információ individualizációját, azt, hogy a készülék használatát, az általuk kedvelt tartalmakat saját ízlésükhöz tudják igazítani.

A fiatalok és az interaktív média

Nemcsak fogyasztók, hanem források is, maguk is részt vesznek a terjesztésben. Ezt a tényt igen előnyösen használta ki kampányában a legutóbbi elnökválasztáskor Barack Obama: fiatal hívei spontán készítettek felvételeket nyilvános szerepléseiről, és feltették a YouTube-ra.

Az aktív, szabad, egyéni médiafogyasztás még inkább lerövidíti a gyermekkort, a felnőttkorba való átlépés, a családból a „külvilágba” való kilépés felületévé válik. A serdülők egyre inkább az interneten keresztül tájékozódnak az őket érdeklő ügyekről. Így például többségük nem veszi igénybe a hagyományos egészségügyi szolgáltatást, hanem panaszkodnak az interneten keresztül keresnek megoldást.

Az internetes kommunikáció fontos szerepet játszik a serdülők értékeinek és egyéniségének kialakításában. Szociális interakcióikat főként azokkal a barátokkal folytatják, akikkel személyesen is kapcsolatban vannak. A kockázatok közé tartozik, hogy a valóságos baráti találkozások száma csökken. Nem kétséges, hogy a médiahatások szerepet játszanak az elhízás, illetve a kóros soványság, az anorexia terjedésében. A robusztus médiahasználat gyakran összefügg a gyenge iskolai teljesítménnyel.

A fiatalok körében különösen népszerűek a közösségi oldalak, amelyek felfutása az elmúlt négy-öt évben zajlott. A korábbi, nemzeti keretek között kialakult közösségi oldalak mára kikerültek az érdeklődés homlokteréből, s helyüket elsősorban az amerikai eredetű, globális Facebook vette át. A Facebook kezdetben a személyiségi jogokat tiszteletben tartó adatkezeléséről volt ismert. Idővel azonban a fiatal alapító sem tudott ellenállni a kísértésnek, hogy átengedje az adatokat üzleti felhasználásra. Emberi jogi képviselők kedvetlenül állapítják meg, hogy a fiatalok gyakran mindenféle aggály nélkül tesznek fel az internetre bizalmas adatokat, intim ügyeket (lásd még Szabó Endre, Talyigás Anikó és Székely Iván fejezetét könyvünkben).

Egyre inkább eldöntött kérdésnek látszik, hogy a médiahatások jelentősen hozzájárulnak az agresszív viselkedés terjedéséhez. A közvetlen hatások mérése azonban nem könnyű, hiszen a számítógép-használat hatása rejtett és kumulatív. A média hasznélvezői által finanszírozott kutatások és szakértői vélemények rendre tagadják ugyan, hogy a durva televíziós vagy számítógépes tartalmaknak közük lehet az agresszív viselkedés terjedéséhez, a közelmúltban egy érdekes hír mégis alaposan megcáfolta ezt a véleményt. A *Heti Világgazdaság* számolt be róla, hogy a Pentagon beszünteti a katonai kiképzéshez használt szimulációs játékok előállítását. Az ok: az agresszív számítógépes tartalmak legdurvább fajtája, a számítógépes játékok megfelelnek erre a célra.

Szó esett már róla, hogy a gyerekek számítógép-használatának szülői, felelős felnőtti kontrollja már kisgyermekkorban is nehézségekbe ütközik, a serdülők esetében pedig gyakorlatilag nem létezik. Ennek következményeként a felnőtt társadalom nem is szerez tudomást arról, milyen honlapokat látogatnak, kivel és hogyan csevegnek vagy játszanak a fiatalok. A közelmúltban egy tragikus eset, egy 17 éves fiú öngyilkossága kapcsán szereztem tudomást egy portálról, amelynek nyomdafestéket alig tűrő elnevezése: „Napiszar – az internet pöcegödre”. Bemutatásként közlöm önmagukról szóló leírásukat:

„Mi az a Napiszar?

Az internet pöcegödre! Itt minden szemetet megtalálsz ami a neten kering. Naponta jelentkezünk friss szarral, hírekkel, képekkel és egyéb gusztustalanságokkal.

Kik kommentezhetnek?

Bárki aki regisztrál. A regisztrációnál beírt adataidat megőrizzük és felhasználjuk mindenféle aljas célra! (buzi hírlevelekre iratunk fel és pénzt lopunk a bankkártyádról!)

Hova talicskázhatom Nektek a szart?

Ide tolhatod : napiszar.com@gmail.com

Nem válaszolunk minden levélre külön. De mentünk minden érdemleges dolgot, és idővel ki is fog kerülni.

Panaszt szeretnék tenni az oldal ellen, mit tegyek?

A polgárjénő hivatalban kell feljelentést tenned, vagy ide írd: polgarjeno@hivatal.hu

A www.napiszar.com egy ritka nívós közéleti magazin! Becsüld meg hogy tagja lehetsz! Látogasd naponta többször és kommentekben káromkodj sűrűn! Az oldalt reklámozd ahol csak tudod!

Jogi blablalba:

Az oldalon szereplő kommentekért felelőséget NEM vállalunk!

Az oldalon megjelent képek, videók, írások a véletlen művei! Ha bármilyen egyezés lenne élő, halott, vagy előhalott emberekkel akkor az kizárt dolog mert nem tudom!”

Ez a szöveg talán tűnhetne egy kicsit durva, de ártatlan ugratásnak, de a portál nem vicces. Nevének megfelelően képből és szövegben bőségesen kínál az ürülékhez kapcsolódó témákat, primitív obszcenitást, a halál és a pusztulás dicsőítését, náci utalásokat, homofób szövegeket. A közönség jellegéről és életkoráról képet alkothatunk a fényképek és videók alapján: egészen fiatal, 14-15 év körüli gyerekek láthatók obszcén pózokban, mutogatják meztelen testüket. A nyilvánosságnak, a felnőtteknek, a szülőknek és a pedagógusoknak fogalmuk sincs a hasonló internetes tartalmak létezéséről, amelyek igenis alkalmasak rá, hogy érzékeny, problémákkal küzdő serdülők állapotát súlyosbítsák. Nem kevésbé kártékonyak azok az internetes portálok és fórumok, amelyek egy egyre szélesebb körben terjedő, nagyon súlyos, gyakran halálos végű lelki betegség, az anorexia támogatására létesültek. Bors Rékának a pro anorexia fórumokról készült tanulmánya rávilágít, hogy e fórumok segítségével a kórosan fogyni vágyó lányok közösségre találnak, miután az egészségükért és életükért aggódó családtagjaikkal, barátaikkal megromlott a viszonyuk. Ez a támogatás azonban nem a gyógyulás, hanem a további állapotromlás felé vezet: a résztvevők ötleteket adnak egymásnak, hogyan lehet hatékonyan súlyt veszíteni, hogyan lehet a környezet előtt titkolni állapotukat. Az internetes kapcsolattartás általában nagyon fontos szerepet tölt be ezeknek a lányoknak

az életében. Az evészavarokkal foglalkozó pszichiáter szerint az anorexiás lányok 90%-a használja a fórumokat. Bár a szerző megállapítása szerint az internetes portálok nem közvetlen előidézői az anorexiának, amely minden esetben komplex problémák következménye, de vitathatatlanul súlyosbítják a betegséget, és megakadályozzák a beteg fiatalokat a gyógyulni akarásban, növelve ezzel a halálos végkimenetel kockázatát. Forgács Attila szintén arra hívja fel a figyelmet, hogy a média alapvető szerepet játszik a táplálkozási zavarok kialakulásában.

A serdülőket fenyegető legfőbb veszély a függőség, az addikció, amely egyre szélesebb körben terjed (lásd kötetünkben Demetrovics Zsolt és Koronczai Beatrix írását). Különösen komoly függőség alakulhat ki a csoportos internetes szerepjátékokat játszóknak között, mivel az akciókat együtt kell bonyolítani, az esetleges kilépő társai sem tudnak tovább játszani. A számítógép-függőség ma már a pszichiátriai diagnosztikában is szerepel, egyre több fiatal küzd különböző formáival.

A gyerekek és a kockázatok

A számítástechnika, az elektronikus kommunikáció léte tehát a hallatlan előnyök és a mindennapi életet segítő hatások mellett igen súlyos kockázatot is jelent, különösképpen a felnövekvő nemzedékek számára. Kérdés: szükséges-e a gyerekek számára védelmet nyújtani a medializált társadalom kockázataival szemben? Ha pedig erre a kérdésre pozitív a válasz, további kérdések merülnek fel azzal kapcsolatban, kinek a felelőssége és feladata a gyerekek védelme.

Azokkal szemben, akik aggódnak, hogy a gyerekek túlságosan fiatal korban kezdik az elektronikus eszközök használatát, gyakran elhangzik az érv, hogy a felnevelkedés során a különböző történelmi korok gyermekeinek mindig az adott kultúra feltételeihez kellett alkalmazkodniuk. A gyermekek „természetes” környezete, a felnőttek által teremtett mesterséges környezet – a civilizá-

ció aktuális állapota – szabja meg, hogy a gyerekek a lovaglásban vagy az autózézetésben szerezhnek-e jártasságot. Ma egyszerűen az elektronikus média mindenütt való jelenléte az, amibe a gyerekek belenőnek. Bayer Judit tanulmányában ezzel kapcsolatban azt emeli ki, hogy a gyerekeknek meg kell tanulniuk a felnőtt világ „farkastörvényeit”, mielőtt szüleik, nevelőik elengedik a kezüket. Az érvelés lényege nemigen vitatható: kétségtelen, hogy a valóság kellemetlen vagy veszélyes oldalait is meg kell ismerniük a gyerekeknek, s valóban nem helyes, és nem is lehetséges hermetikusan elzárni őket. Bayer Juditnak az a feltételezése azonban, hogy a gyermekek természetes immunitással rendelkeznek a kártékony tartalmakkal szemben, nem felel meg a pszichológiai tényeknek. Fizikailag is kímélni igyekszünk a fejlődő gyermekeket, így mentálisan is arra van szükség, hogy fokozatosan vegyék fel a terheket, amelyeket felnőttkorukban el kell vinniük. A védettség hiánya testileg és lelkileg is próbára teszi a gyerekeket: ne feledjük, a történelem más korszakaiban csak töredékük érte meg a felnőttkort. Sokan nem bírták ki a tisztaság hiányát, a durva fegyelmezést, azt, hogy kicsi koruktól keményen dolgozniuk kellett. A XIX. századi Angliában gyermekek tízezrei váltak nyomorékká, mert a gyári munka miatt túl keveset tartózkodtak a napon, és nem erősödtek meg a csontjaik (nem véletlenül nevezték angolkórnak is ezt a betegséget). A gyerekek felnevelkedése nem önszabályozó folyamat, nincs semmiféle korrekciós mechanizmus, amely a kedvezőtlen nevelési körülmények hatását kiküszöbölné. Ráadásul a következmények csak évek, évtizedek múltán jelentkeznek, amikor a változások lényegében már visszafordíthatatlanok.

A gyermekkort a modernizáció „fedezte fel”. A felfedezés valójában nem a gyermekkorra, hanem a gyerekek különleges tulajdonságaira vonatkozott. A modernizáció által teremtett körülmények tették lehetővé a gyermekkor és a felnőttiség elkülönülését, különleges feltételek megteremtését, amelyek lehetővé tették a gyerekek számára, hogy életük első, mintegy másfél évtizedében ne szembesüljenek a felnőtt világ durvaságával és nehézségeivel.

Ne kelljen – legalábbis a fejlett világban – zsenge korukban pénzt keresniük, ne használhassák ki őket a felnőttek, ne élhessenek vissza tapasztalatlanságukkal, kiszolgáltatottságukkal. Ebben a kontextusban kell értelmeznünk azt a valóságot, amelynek egyik legfőbb komponense az elektronikus kommunikáció és a média.

A társadalmi kommunikáció fajtái történelmünk során nemcsak az általuk közvetített tartalmak tekintetében különböztek, hanem abban is, hogy a közönség milyen szegmensei számára voltak képesek tartalmakat közvetíteni. A mai kommunikációs eszközök teljességgel egyedülállóak abban, hogy üzeneteiket egy adott társadalom szinte minden tagjához képesek eljuttatni, társadalmi rétegtől és – ami itt számunkra fontos – életkortól függetlenül.

2010 tavaszán megdöbbentő hír foglalkoztatta a közvéleményt. Egyik napilapunk „Hétvége” melléklete arról adott hírt, hogy Németországban fontolgatják a pornográfiával foglalkozó iskolai tantárgy bevezetését.⁴ A józan ítéletű olvasók aligha értenek egyet a cikkben megszólaló kollégáimmal, akik támogatnák a tervet. Ha a hír nem csupán az olvasottság növelését serkentő kacsza, és valóban megpróbálkozik valaki a pornográfia tantárgy bevezetésével, az feltehetően igen erős lakossági ellenállásba fog ütközni. Az ötlet ugyanakkor világosan jelzi a súlyos csapdahelyzetet, amely a média és a társadalom kapcsolatában mára kialakult. Miközben a tömegkommunikáció folyamatosan megújuló eszközei alapjaiban formálták át a mindennapi élet minden létező szegmensét az intézmények és a politika működésétől az emberi érintkezésig, a média – csakúgy, mint a pénzpiac – teljes mértékben kívül került a társadalmi irányítás eszközrendszerén. A rendkívüli befolyás, amelyre a mai tömegtájékoztatás szert tett, több oldalról is „be van biztosítva”. Többek között hatékony ideológiákkal, amelyek mögé némi naivitással gyakran odaállnak a progresszió lelkes hívei. Holott a szólásszabadság bárminemű korlátozásának ellenségei közül jó néhányan nem független szabadgondolkodók, hanem nagyon is jól követhető anyagi érdekek mentén cselekszenek. Valójában természetesen a szólásszabad-

ságnak mindenütt vannak korlátai: pedofil tartalmat nem lehet közzétenni, és a legtöbb országban törvény tiltja a nyílt náci/fasiszta uszítást. Megengedett ugyanakkor embertársunkat ölésre, öngyilkosságra, bombakészítésre biztatni és tanítani, ha ehhez nem járul artikulált ideológiai tartalom – mintha nem volna önmagában is ideológiai tartalma annak, amikor valaki bármilyen módon is támogatást nyújt életek kioltásához.

A gazdaság és a politika más ágaival szorosan összefonódott a tömegtájékoztatási ipar. Létező eszköz a gyógyszergyárak mintájára olyan szakértők és kutatások bőkezű finanszírozása, akik és amelyek konzekvensen tagadják a legnyilvánvalóbb összefüggéseket. Ez történt a képernyőn látható agresszió viselkedésre gyakorolt hatásával. Miközben a hétköznapi gondolkodás számára is teljesen triviális, hogy a természetes agresszió megtapasztalása növeli az agresszív viselkedés esélyét, folyamatosan születnek újabb „kutatások”, amelyek az összefüggést kétségbe vonják.

Valójában tehát a társadalomnak ma semmiféle befolyása nincs a média működésére vagy az abban szereplő tartalmakra, miközben a kockázati lehetőségek semmivel sem kisebbek, mint az élelmiszer-biztonságban keletkező rések (amelyek szintén egyre kontrollálhatatlanabbak). Ez a kínos csapdahelyzet fejeződik ki az olyan bizarr elképzelésekben, mint amilyen a pornográfia tantárgyként való bevezetése az iskolában. A gyerekeket ugyanis kétségtelenül nem lehet biztonságosan megóvni attól, hogy az interneten bármikor a legdurvább természetes, pornográf tartalmakra bukkanjanak, miközben a legtöbb ember meggyőződése szerint ez nem tesz jót a gyerekeknek. Ezen csak a nyilvánosságra hozatal korlátozása segíthetne. Ismert: anyagi érdek, például a szerzői jog védelmében lehet korlátozni tartalmak közreadását. Ha azonban a tartalmak nem üzleti célú és nem a kitüntetett területet érintő (pedofília, holokauszttagadás) korlátozása szóba kerül, a fejlett országokban egyes szószólók rögtön diktatúráról és a szabadságjogok súlyos korlátozásáról beszélnek. Nem merül fel értéksorrend, az előnyök és a hátrányok mérlegelése: a tömegtájékoztatás korlátozása bizonyos témákat kivéve gyakorlatilag tabu.

Mit lehetne tenni ilyen körülmények között, ha mégis szeretnénk megkímélni a gyerekeket a korai kiábrándulástól, elfásulástól? A megoldás az egyénre, a szülőkre és a gyerekekre hárul: vértézzük hát fel magukat a gyerekeket az őket károsító tartalmakkal szemben. Csakhogy a probléma éppen az, hogy ők képtelenek erre ugyanúgy, ahogyan sem úszni nem tudnak maguktól, sem azt nem tudják, hogy az éles késsel megsérthetik magukat. Némi cinizmussal mondhatjuk, hogy a kártékony tartalmak, így a pornográfia megismerésének kötelezővé tétele hatékony volna, mivel így a gyerekek már idejekorán fásulttá és közömbössé tehetők a hasonló tartalmakkal szemben.

A pornográfia tantárgyként való bevezetése egyfajta pótcselekvés, amelynek legfőbb előnye, hogy elkerülhetővé teszi a problémával és annak gyökereivel való nyílt szembesülést. Követi a posztmodern kultúrában terjesztett mítoszt, amely szerint a döntések valójában az egyének kezében vannak, ha megfelelő módszertan és technika segítségével felvértézzük őket. Ez az ellentmondás már a televízióra vonatkozó tartalomszabályozás esetében is megjelent, de minden bornírtsága ellenére töretlenül használják évek óta: bizonyos filmeket az adott korhatár alatt a gyerekek csak „nagykorú felügyelete” mellett nézhetnek. Vajon hogyan tudná megóvni a „nagykorú” a gyerekeket az elborzasztó vagy rémisztő látványtól? Az esetleges kommentár legfeljebb tompíthatja a hatást, de képzeljük csak el a mindennapi életben azt a helyzetet, amikor a gyerekek és a szülők együtt néznek valamit, és a szülő folyamatosan magyarázatokat fűz a látottakhoz. A média rendkívüli gazdasági és politikai erejét tükrözi, hogy ezzel a nevetséges kompromisszummal kellett megelégednie a szabályalkotónak, még azt sem érte el, hogy az adott filmeket egyszerűen ne ajánlják egy adott korosztály tagjainak (ami nem tiltás!).

Jordan amerikai kutató arra hívja fel a figyelmet, hogy szólásszabadságnak az Alkotmány első kiegészítésében szereplő elve gyakran szembekerül a gyermekek védelmének követelményével. Amikor új médiaszabályozás készül, a társaságok megígérik az önszabályozást, az azonban, hogy valóban betartják-e,

teljességgel ellenőrizhetetlen. Ilyen például a korosztályi besorolás, ami mindig valamilyen nyilvános felháborodást vagy intézkedéstervet követ. Más esetekben a médiatársaságok látszólag betartják a törvényt, de csak annak betűjét, nem a szellemét. Például az Egyesült Államokban a gyártás során beszerelték a televíziókészülékekbe az úgynevezett V-chipet, amelynek segítségével a szülők meg tudták akadályozni, hogy gyerekeik bizonyos csatornákat nézzenek, de bekapcsolása bonyolult, és a szülők többsége nem is tudott a létezéséről. A legtöbb csatorna betartja a szövetségi állam azzal kapcsolatos előírását is, hogy naponta három órán keresztül kifejezetten didaktikai célú műsort sugároznak, ám ezek a műsorok gyakran egyáltalán nem vonzóak, vagy valójában nem gyerekeknek valók. A szülői kontrollt különösképpen megnehezítik a médiatechnológia gyors változásai. A szülők nem értik, hogyan használják gyerekeik a médiát, a gyerekeket kéri meg, hogy programozzák be a televíziót, mutassák meg, hogyan működik a mobiltelefon. Nem ismerik a gyerekeik által használt portálokat, interaktív játékokat.

A letölthető szűrőprogramok sem jelentenek megoldást: legfeljebb 8-10 éves korig alkalmasak a gyerekek megóvására, az ennél idősebb gyerekek már biztosan megtalálják a módját, hogy elérjék az őket érdeklő tartalmakat. Nem életszerű Bayer Judit megállapítása, amely szerint a gyerekek, ha nekik való oldalakat találnak az interneten, kevésbé fognak érdeklődni a felnőtteknek szóló tartalmak iránt. A gyerekekre mindig is nagy vonzerőt gyakorolt az, ha valami nem nekik, hanem a felnőtteknek való volt. A számítógép-használat szülői kontrollja kivitelezhetetlen, és nemcsak a már említett technikai problémák miatt. A serdülők többsége számára a szülők véleménye sokkal kevésbé fontos, mint társaiké, az internetes portálok fórumain megszólalóké.

Az állam nem szólhat bele az egyének médiafogyasztásába, nem döntheti el, mi a jó a gyerekeknek és mi nem – vélik többen. Csakhogy az állam intézményeket tart fenn a gyerekek számára, tanterveket és működési szabályokat készít, normákat állít fel a neveléssel kapcsolatban. Ezen túl külön intézményrend-

szer, a gyermekvédelem létesült annak érdekében, hogy bizonyos helyzetekben az állam megvédje a gyerekeket akár saját szüleikkel szemben is. Az „állam” egyébként meglepően sok dologba szól bele: törvény tiltja, hogy a szülő testi fenytést alkalmazzon. Szabályok írják elő, mekkora ketrecben lehet sertést tenyészteni, hogyan szabad libát etetni. Elvileg tehát megvolna a lehetőség a média szabályozására, ráadásul erre nemcsak hatósági, hanem piaci jellegű eszközök is rendelkezésre állnak. A frekvenciák tulajdonosa ma is az állam, eldöntheti, melyik csatorna részesül belőle. A szabályozás hiánya nem elvi lehetetlenség, hanem az aktuális hatalmi viszonyok tükröződése. A kontroll nélküli médiatársadalomban való felnevelkedés következményei nem lesznek olyan látványosak, mint a pénzügyi szabályozatlanság okozta gazdasági válság, de a hatásuk még súlyosabb lehet.

EMBER A VÉGTELEN TÉRBEN EGYKOR...

Az ég egy sátor, melyet az ősök által lenyúzott kenguru kifeszített bőréből készítettek, széleit faékekkel kifeszítették, majd felemelték. Miután az ősök elvégezték munkájukat, megelégedve mondták:

„Mostantól kezdve az emberek egyenesen járhatnak, s nem kell elrejtőzniük attól félve, hogy az ég leesik.”

AZ AUSZTRÁLIAI NAGAMENI TÖRZS ELBESZÉLÉSE (Láng, 1979)

Szabó György Mérnök, térinformatikus, a tér regisztrálásával, modellezésével kapcsolatos interdiszciplináris területek szakértője, szakkönyvek, tanulmányok szerzője, a Budapest Műszaki és Gazdaságtudományi Egyetem docense

VIRTUÁLIS VILÁG ÉS VALÓS TÉR. UTÓPIÁK, REALITÁS, VESZÉLYEK

A körülöttünk lévő világ tárgyainak, jelenségeinek valóságghú ábrázolása, a környezet viszonyait visszatükröző modell megalkotása az emberiség régi vágya. Az épített világ és a természet világának térbeli megismerése, modellezése, ábrázolása a korai civilizációktól napjainkig számos szakterület alapfeladata.

Az internet széles körű elterjedése és a helymeghatározás technológiájának egyszerűsödése jelentősen megemelte a térbeli adatok alkalmazásának mennyiségi, minőségi elvárásait. További jelentős változást hozott a civil felhasználók megjelenése a napjainkig alapvetően stratégiai eszközként kezelt helymeghatározás, térképészet világában. Ez felborította az eddigi szigorú szakmai alkalmazások szokásrendjét.

A digitális, térbeli adatkészletek megjelenésének hatására a tudományos kutatás és a műszaki fejlesztés súlypontja eltolódott az adatnyerésről az adatok széles körű hasznosításának irányába. A digitális képkalkoló rendszerek, műholdas helymeghatározó rendszerek és mobil mérőrendszerek megjelenése ezen a téren is forradalmi változást hozott.

A vizsgált térbeli jelenségek területi kiterjedése, fogalmi definíciója, térbeli-időbeli felbontása a papír alapú dokumentumok világában megszokott statikus jelleg helyett dinamikus modellé vált. A térképészet, az informatika és a geotudományok határterületén kialakult a térinformatika.

A kezdeti örömök után a felhasználók szembesültek:

- a digitális térbeli adatok automatikus regisztrálása nyomán keletkezett adathegyek befogadási, értelmezési problémáival;
- a körülöttünk lévő világban lejátszódó bonyolult folyamat megértéséhez szükséges, összetett elemzésekkel;
- a ténnyel, hogy mint mindennek, az információnak is ára van. Az információ sajátos gazdasági költség szerkezete elrejteti azt a tényt, hogy az „ingyenes” információ felhasználásért – többek között – időnkkel, személyes adatainkkal, fogyasztói elkötelezettségünkkel, kiszolgáltatottságunkkal fizetünk.

A hétköznapi felhasználóktól a közelmúltig elzárt térképészeti, térinformatikai világ eszközeinek napi használatát a felmerülő jelentős igény ellenére még további körülmények nehezítik:

- a virtuális modellek csak igen durva absztrakciói a valóságnak, így ezek többnyire csak a készítő aktuális igényeit elégítik ki maradéktalanul;
- a létrehozott térbeli modellek használatát a valóság nemzetbiztonsági szempontok miatti megmásítása jellemezheti;
- előfordul a szándékos megtévesztés, amelyet a pillanatnyi üzleti érdek vagy a rosszindulat motiválhat.

Az ember és a tér

A tér és a térben lejátszódó jelenségek feletti uralom biztosításának érzete, illúziója alapvető emberi, társadalmi igény, amelynek megléte egyfajta szubjektív biztonságérzetet nyújt az egyének vagy szervezetnek. Az emberiség őstörténetétől napjainkig a térbeli biztonságérzet elvesztése veszélyérzetet, szorongást generál. Ilyenkor a veszélyérzet kivédésének legfontosabb eszköze az ember térbeli viszonyának megismerése. Az iparágak széles skálájára jött létre az egyén és embercsoportok biztonságérzetének kielégítésére a turisztikai tájékoztatástól a hadászati felderítésig.

A valóság uralásának ígéretét nyújtó térbeli modellek hasznosságát a gyakorlat igazolja: lásd a mottóban szereplő nagame-ni törzs kifeszített kengurubőrből készített égboltját vagy a görög mitológia Atlasz¹ által tartott eget.

A térbeli adatok mérésének és ábrázolásának technológiai nehézségei és jelentős költsége magyarázzák, hogy a térbeli kontroll csak lassan terjedt a globális szintekről a regionális, lokális mikroterekre. Ezzel ellentétes utat járt be az egyének által megismerhető tér, amely a mikroterektől a lokális, regionális, globális terek irányába halad.

A térképészeti, térinformatikai adatok stratégiai jellege miatt szinte minden kultúrában megjelenik a dilemma a térbeli adatok nyilvánosságának nemzetbiztonsági érdekből történő korlátozása és az egyének saját térbeli adataikkal való információs önrendelkezésének korlátozása között. Kinek a tulajdonát képezi az én térbeli pozícióm? – tehetjük fel a kérdést.

Emberöltökön keresztül az állam hatékonyan gyakorolhatta a térbeli adatkezelés monopóliumát, mert pontos térbeli adatok előállítása, karbantartása, ábrázolása csak igen nagy szervezettségű és erőforrásokat hosszú távon biztosítani tudó szereplők számára volt lehetséges. A képi adatnyerés, a mesterséges holdakon alapuló globális helymeghatározás és a mobil helymeghatározást lehetővé tévő technológiák (GPS, GSM, WIFI, RFID) széles körű üzleti elterjedése azonban már az adott technológia szolgáltatója és felhasználója

számára is lehetőséget nyújt a térbeli adatok tömeges, olcsó begyűjtésére, tárolására, elindítva ezzel a korlátok közé nehezen szorítható adatfelhasználást, adatkereskedelmet ezen a területen is.

A térbeli adatgyűjtés, ábrázolás – egy kis technikátörténet

A földmérés, a térképészet mint a valós világról történő ismereteink strukturált gyűjtésének, rendszerezésének és közlésének eszköze évezredek óta szolgálja a körülöttünk lévő világ jelenségeinek megismerésén, elemzésén, modellezésén fáradozó társtudományokat. A térkép – mint említettük – évezredekken keresztül csak kevés kiválasztott által birtokolt, használt „stratégiai fegyver” volt. Ezt az egyediséget törte meg a sokszorosítás, a nyomdatechnika megjelenése. A térkép a környezetünkkel kapcsolatos vizuális kommunikáció általános eszközévé vált. Ez az analóg ábrázolás az évezredek során létrehozta a térképek nyelvét, a valós világ jelenségeinek, helyzetének, alakjának, a terep domborzatának ábrázolási szabályait.

Eltérő térbeli információs igényekkel jelentkezik az adózás, a honvédelem, a kereskedelem, a hajózás, a navigálás – és folytathatnánk a sort. Az igen drága eseti mérésekkel szemben elindították az adott térség, jelenség általános célú rendszeres felmérését és ábrázolását. Az így kialakult és mind a mai napig használt általános és szaktérképek – navigációs, kataszteri, katonai térképek – rendszere a térképi nyelv számos „dialektusát” alakította ki, nehezítve az általános felhasználók számára azok megértését.

A környezeti adatgyűjtés egyszerűsítése, a földfelszín madárperspektívából való megfigyelése az ember régi vágya volt. A levegőből történő adatgyűjtésnek az ember által irányított első ballonnal történő megvalósítására 1783-ban került sor. A képi információ alapuló adatgyűjtési eljárás, a fotogrammetria (fényképmérés) elméleti alapjait Lambert² még a fényképezés feltalálása előtt publikálta. A fényképezés feltalálása (1839), amely Louis-Jacques-Mandé Daguerre nevéhez fűződik,³ megteremtette az adott kör-

nyezeti feltételek között, a tér egy adott nézőpontból szemlélhető látványának objektív leképezését biztosító eszközt.

A fényképezés megjelenése után hamarosan sor került az első távérzékelési kísérletre a Gaspard Felix Tournachon⁴ által 1858-ban ballonról elkészített fénykép formájában, megalapozva a topográfiai térképezés új technológiáját. Az első mesterséges hold 1957-ben történt felbocsátása elindította az űrtávérzékelés fejlődését. Az első egyszerű fényképtől napjaink elektro-optikai képalkotó rendszeréig technológiák tömegét fejlesztették ki.

Az optikai képi információfeldolgozás korlátaival már a XX. század közepén szembesültek. A képalkotás technikája (radar), a fokozott pontossági igények (térképészet) és a képi információk nagy mennyisége (távérzékelés) miatt az analóg feldolgozások nem feleltek meg a kor elvárásainak. Elkerülhetetlenné vált a képi információ digitalizálása. A digitális tárolás alapeleme a képi információt hordozó elemi jel, a pixel.

A téri tájékozódás – tér, idő, hely

Környezetünk térbeli viszonyai, a természeti, infrastrukturális, gazdasági, társadalmi jelenségek területi eloszlásának egyenlőtlenségei az elmúlt emberöltők során alapvetően meghatározták az adott földrajzi hellyel kapcsolatos lehetőségeinket. Az emberi tevékenységeknek ez az erős helyfüggése szinte természeti törvényként hatotta át múltunkat, történelmünket. Az eltérő földrajzi helyeken jelentkező előnyök egyoldalú „lefölözését” a helyváltoztatás időparamétere határozta be.

Az infokommunikációs technológia által létrehozott virtuális világ logikája átlépi ezeket a merev határokat, a távolság eliminálásával, a távoli helyek közötti egyidejűség megteremtésével kitágítja a földrajzi helyhez kötött tevékenységek kereteit.

A közönséges halandók is lehetőséget kapnak az idő korlátainak legyűrésére, a tér és idő mint alapvető erőforrások feletti kontroll megszerzésére.

A tér jelenségeinek regisztrálása és problémái

A bennünket körülvevő tér objektumainak, jelenségeinek modellezése mind a mai napig komoly kihívást jelent a környezet formálásában (mérnökök, művészek, társadalomtudósok) és a tér regisztrálásában szerepet játszó szakemberek (geodéták, térképészek, térinformatikusok) számára.

A térkép formájában létrehozott ikonikus vizuális modellt a „valóság kicsinyített másaként” interpretálták, amely alapvetően a „mi volt?”, esetleg a „mi van?” kérdésre kívánt válaszolni.

A térinformatika világában a statikus megjelenítést felváltotta a valós idejű megjelenítés, ahol a megválaszolandó kérdés a „mikor?”, „hol?” „mi van?”.

Egyre jelentősebb szerepet kapnak a térbeli viszonyokat nagy geometriai hűséggel leíró (esetenként már a folytonos mintávételezés ígéretét nyújtó) háromdimenziós komplex modellek. A térinformatika felhasználóinak azzal az abszurd helyzettel kell napjainkban megbirkózniuk, hogy nagyobb tömegű bit és koordináta áll esetenként rendelkezésre egy-egy térbeli feladat megoldása során, mint amennyit értelmesen hasznosítani tudnak.

A már említett és napjainkban széles körben elterjedt új helymeghatározási és regisztrációs technikák (GPS, GSM, WIFI, RFID, képalkotó rendszerek) lehetőséget biztosítanak akár egy egyén vagy nagyobb embercsoport napi útvonalának, tevékenységének rendszeres regisztrálására. Az így létrejött tér-idő utelemzések több egyén esetén lehetőséget adnak az egyének közötti tranzakciók elemzésére, az idők átfedése alapján az adott helyen történő egyidejű jelenlét detektálására (lásd a kérdés más megközelítéseit Székely Iván kötetünkben közölt írásában).

Hazai viszonyok között egy átlagos esztendőben húsz-harminc légi fényképezésre alkalmas nap van, ami megnehezíti nagyobb térségek jó minőségű állapot rögzítését. A térképészeti minőségű légi fényképezés nemzetbiztonsági okokból légicenzori felügyelet alatt folyik, így bizonyos objektumokról csak a titkos ügykezelés betartásával kaphatunk légi felvételeket. A távérzé-

kelési technológiák napjainkban lassan lefedik a hagyományos fotogrammetriai térképészeti pontossági igényeket is.

Alapvető különbség a szenzorokkal előállított adatokhoz való jogi és üzleti hozzáférésben van. A távérzékelési műholdak többnyire erős nemzetbiztonsági kontroll alatt működnek, még a kereskedelmi szolgáltatók is tolerálják a politikai realitásokat. Például az Egyesült Államok kormányának kérésére a kereskedelmi műholdszolgáltatók nem értékesítenek két láb (kb. 60 cm) mértéknél nagyobb felbontású adatokat, de egy lokális fotogrammetriai alkalmazásnál csak idő, pénz és tárolókapacitás kérdése az akár három centiméteres felbontású képanyag készítése. Az adatokhoz kapcsolódó felhasználói jogokban is lényeges a különbség. Míg fotogrammetriai módszereknél a felhasználó a saját igényei alapján előállított adatok tulajdonjogát is megvásárolhatja (ez a gyakorlat), addig a távérzékelési alpanyagoknál a szolgáltató szervezetek a rendszeresen gyűjtött adatok egy részhalmozásának adott feladatban történő felhasználási jogát értékesítik.

Napjaink mobil mérőrendszerei a különböző helymeghatározási, adatgyűjtési technológiák integrációjával jöttek létre. A földi, légi vagy műholdplatformon integrált mobil mérőrendszer helymeghatározó komponense egy GPS, IMS, GSM vagy WIFI eszköz, képalkotó része digitális kamera, videokamera vagy lézerszkennerek. Az így integrált eszközrendszer lehetővé teszi a környezet háromdimenziós geometriai modelljének közel valós idejű leképezését, a hagyományos módszereknél jelentősen nagyobb frissítési frekvenciájú modellek létrehozását. A mobil mérőrendszerek gyorsaságát és pontosságát beárnyékolja az így előállított adatkészletek nagy költsége és a direkt mérési technológia miatt az adatok környezeti zajokra, elektronikus zavarásra való fokozott érzékenysége.

Valós és virtuális terek – statikus, dinamikus, mobil modellek

Az elmúlt évtizedek technológiai fejlődése kiszorította a hagyományos térképkészítő, környezetleíró, gyakran emberöltős adatfrissítési ciklust biztosító módszereket. Ezzel együtt a helyzeti adatok előállítási költségeinek rohamos csökkenése is bekövetkezett, ami lehetővé teszi a környezeti viszonyokat leképező hagyományos térbeli adatbázisaink évi, havi, heti, napi, napon belüli aktualizálását, az időbeni változások nagy gyakorisággal történő követését.

A természeti és épített környezet „statikus” viszonyait leíró hagyományos topográfiai tartalom mellett megjelenik a kis időtávon is gyors változásokat elszenvedő „dinamikus” tartalom (például időjárás, légszennyezés) és a folyamatos frissítést igénylő „mobil” tartalom (például forgalmi viszonyok, parkolók foglaltsága, barátaim aktuális tartózkodási helye) (lásd a közösségi portálokról e témában írtakat Rácz Bencze, Szabó Endre és Talyigás Anikó fejezetében).

Napjainkban a virtuális világ, intelligens város, *cyber city* fogalmakat a valóságon messze túlmutató, teljesen esetleges jelentéssel felruházott fogalomként alkalmazzák az információs társadalom különböző szereplőinek fogalomtárában.

A valós világ modellezését megkísérlő virtuális világokat az alábbi csoportokba oszthatjuk:

1. A digitális világba történő belépés legegyszerűbb eszközei az interneten közvetlenül elérhető tájékoztató portálok, turisztikai kalauzok, menü- és egydimenziós linkjegyzékek. Alapvető funkciójuk az adott térség iránt érdeklődő felhasználók reklámmal, turisztikai információkkal való ellátása.

2. A kétdimenziós modellek az adott térséget madárperspektívából ábrázolják, alapvető funkció az adott térségben lévő érdekes pontok, helyek felé való csatlakozási terület biztosítása a térképen elhelyezett 2D hiperlinkek segítségével.

3. A háromdimenziós modellek az adott térség objektumainak, jelenségeinek 3D geometriai modell formájában történő megjelenítését biztosítják. (Professzionális alkalmazásoknál a 3D

modellek fő célja a tervezés, a szimuláció, a térbeli elemzés ki-
szolgálása.)

4. Az intelligens modellek a felhasználók számára nem csak az egyszerű információelérés vagy látvány élményét nyújtják, hanem a környezeti viszonyok, szolgáltatások és kapcsolatok kezelésére alkalmas felületükkel lehetőséget biztosítanak interakciókra.

5. A kiterjesztett valóságelvű modellek a valós térben mozgó mobil felhasználók számára vetítik rá az okostelefon képernyőjén a virtuális tartalmat (például eladó lakások rávetítése az utca-
képre, egyetemi campus épületeire a keresett tanszék rávetítése).

Hol vagyok én, és hol van, amit/akit keresek?

A mobilitás és a digitális város eszméivel átítatott felhasználó tér-
beli helyzetének és az általa elérni kívánt helyfüggő tartalomnak
valós idejű, personalizált elérését igényli. Az információs társas-
adalommal kapcsolatos pozitív ígéretek halmazában hajlamosak
vagyunk a tér, idő, hely regisztrálását biztosító globális, regioná-
lis, lokális helymeghatározási módszerek korlátainak, technikai
nehézségeinek figyelmen kívül hagyására. A mobil pozíciómeg-
határozásra rendelkezésre álló műszaki megoldások⁵ alkalmazá-
si lehetőségeit befolyásolja az a tény, hogy a helymeghatározást
biztosító fizikai adatokat a passzív fogadófunkciójú mobil eszköz
(GPS) vagy pozicionálási és kommunikációs szolgáltatásokat
egyaránt biztosító hálózat (GSM, RFID, WIFI) fogadja.

A mobil navigáció lázában égő felhasználók hajlamosak figyel-
men kívül hagyni, hogy navigációs készülékük megvásárlásakor
nem szerezték meg a felügyeleti jogot a műholdak és a földi irányí-
tó központ fölött. A rendszer kezelői nemzetbiztonsági okokból bár-
mikor korlátozhatják a szolgáltatások elérhetőségét és a szolgáltatás
pontosságát. További gondokat okozhat az a tény, hogy a GPS-rend-
szer által szolgáltatott műholdjelek viszonylag egyszerű eszközök-
kel zavarhatók, blokkolhatók, ellehetetlenítve a navigációs alkal-
mazásokat. Napjainkban bekövetkeztek az első olyan bűncselek-

mények, amelyek során a professzionális műszaki ismeretekkel és eszközökkel felvértezett bűnözőcsapat a GPS-műholdak kommunikációs frekvenciáját nem zavarta, hanem manipulálta, értékes rakományú kamionokat térítve le útjukról és ejtve csapdába.

A hálózat alapú helymeghatározási technológiák⁶ esetén a helyzeti pontosság a hálózat bázisállomás-sűrűségének függvénye (pl. 50–500 m belterületi, 500 m–5 km külterületi pontosság GSM-hálózatban). Jelentősen hátráltatja az említett technológiák tömeges felhasználásának elterjedését a hálózati csomópontok helyzetének, paramétereinek gyors, eseti változása, az adott szolgáltatás üzemeltetőitől való erős függés.

Megállapíthatjuk, hogy a technológiai fejlődés által megteremtett új eszközök és a mobil infokommunikációs hálózatok segítségével – mint a fejezet elején utaltunk rá – a közönséges halandók is lehetőséget kapnak az idő korlátainak legyűrésére, a tér és az idő mint alapvető erőforrások feletti kontroll megszerzésére. E gondolatot azonban az elmondottak alapján pontosítanánk: az egyszerű, megbízható, olcsó, biztonságos tértechnológia még kidolgozásra vár.

Napjaink tendenciái, veszélyei

Az egyre dinamikusabban fejlődő térinformatikai alkalmazások piacán jelentős fejlődés történt a térbeli adatkészletek elérhetősége, pontossága, aktualitása tekintetében. A kedvező képet némileg beárnyékolja az a tény, hogy a térbeli adatgyűjtés és a térbeli adatokkal való gazdálkodás robbanásszerűen terjed ki a mikro- és személyes terekre. Az információs társadalom polgára gyakorlatilag folyamatos követés alatt áll (lásd kötetünkben Székely Iván írását). Az elektronikus fizetés, a GSM, WIFI, RFID, GPS, földi és műholdas képi adatgyűjtő rendszerek, térfigyelő kamerák szinte minden lépésünket regisztrálják. A téradatpiacra belépő világcégek nem kívánt fotókkal sértik meg az állampolgárok személyes terét. A térinformatikai piac jelentős üzleti sze-

replőli a nagyobb stratégiai súlyú kormányzati tényezők kérésére manipulálják a „valóságot” – a szemünknek sem kell hinni minden esetben a Google vagy a Microsoft által üzemeltetett digitális glóbuszokon keresgélve.



1. ábra. Mi a valóság? – A Google Maps és a Microsoft Bing Maps „kreatív megoldása” egy nemzetbiztonsági okokból álcázandó objektum eltüntetésére



2. ábra. Mi a titok? – A Google Maps 2008. augusztus 30-i és 2009. július 30-i képe Gödöllőről

A 1. ábra bal oldalán egy holland objektum Google Mapsben történő, nem túl sikerült álcázását szemlélhetjük meg. A képretusáló szakember nem fárasztotta magát a környezetbe jól illeszkedő, random jellegű erdőtextúra bemásolásával, helyette egy erdőfoltot mint kitöltési mintát kilencszer másolt az álcázandó objektum fölé. Mint az ábra másik felén megsemlélhetjük, a Bing Maps grafikus már jobb munkát végzett.

A Google által kormányzati kérésre elkövetett módosításokról – bizonyos korlátozásokkal – a <http://www.google.com/governmentrequests/> címen tájékozódhatunk. Az előző mondat-

ban szereplő „bizonyos korlátozásokra” szemléletes példát mutat a 2. ábra. A Gödöllőn elhelyezkedő objektum nem szerepel ugyan a Google nyilvántartásában, de érdekes módon a 2008. augusztus 30-án még a valóságot ábrázoló képet a 2009. július 30-i állapotot ábrázoló felvételeken már kifedték.

A földrajzi azonosítóval ellátott (geo-tag) személyes adatok térbeli személyiségtérkép konstruálását teszik lehetővé. Japánban már megszületett az a szolgáltatás, amely a bértakarítást végző cég alkalmazottainak övére csatolt okostelefon által rögzített pozíció és gyorsulásadatok kiértékelésével a takarítás, helyváltoztatás, pihenés jellemző mozgási szekvenciáinak adatbázisára építve megmondja, hogy az illető alkalmazott valóban felkereste-e az adott helyszíneket, és ott mennyi időt töltött sepregetéssel, ablaktisztítással, felmosással, kávézással.

A nemzetbiztonsági érdekekre való megalapozatlan hivatkozás a térbeli adatokhoz való adathozzáférés monopóliumának megteremtését teszi lehetővé. A terrorizmus elleni harc ürügyén a demokratikus országokban is gyakorlattá válik a személyes térrel kapcsolatos információs önrendelkezés korlátozása.

Az információtechnológiát körüllegő kultusz veszélyeire az elmúlt évtizedek alatt többen felhívták a figyelmet. Minden létező jelenség adatainak digitális formában történő regisztrálását és visszakeresését számítógépeink valóban nagy hatékonysággal képesek megoldani, de ezt tudásként vagy gondolkodásként interpretálni talán túlzás. A napi gyakorlatban elképesztő mennyiségben generálódó digitális adattenger Chaplin *Modern idők* című filmjében látottakhoz hasonlóan maga alá temeti az embert.

„Ha megpróbáljuk az információs technikát megmenteni és emberi célokra használni, egy ponton szembe kell néznünk azzal a kellemetlen ténnyel, hogy a számítógép nagyon is hajlamos a demokratikus értékek aláásására. Ez a veszély éppen abból a képességéből ered, melyet a reklámok állandóan emlegetnek, hogy az információkat begyűjti és ellenőrzi...”⁷

Ember a végtelen térben napjainkban

Szó szerint bevitte a „sűrűbe” a navigációs rendszer azt az észtkamionost, akinek kiszabadításához a hansági lápból egy kamionmentő, két traktor és négy ember megfeszített munkája kellett:

„Az észtkendszámú, nyersanyaggal megrakott Scania nyerges vontató éppen Fertődre tartott, amikor Jánossomorjánál eltévedt. A sofőr – elmondása szerint – még nem járt erre, a navigációs rendszeren pedig vélhetően a legrövidebb útvonalat állította be. A rendszer a tervezéskor valószínűleg figyelembe vette a gyalogos és kerékpáros utakat is, így a Hanság kellős közepére irányította a kamiont. A mintegy 40 tonnás, megrakott járműszerelvény Jánossomorján tért le a 86-os főútról, majd a kisváros közepén rákanyarodott egy földútra. Azon körülbelül hat kilométert haladt, míg aztán arról is letért az ottani vízzel teli csatornák közé, ám ekkor már megfordulni nem tudott. Végül pedig a lápos területen megsüllyedt és elakadt. A kamion ekkor már több mint tíz kilométerre volt minden lakott területtől, az észtksofőrnek pedig fogalma sem volt arról, hol is van pontosan. A férfigyalog indult segítségért. Napokig bolyongott és »ettette« a szünyogokat a Hanság közepén. Végül szerencsére visszatalált a járművéhez, és néhány nap után segítséget is szerzett.”

(www.kisalfold.hu, 2010. 07. 01.)

Turchányi Géza *Tanácsadó, az egyik ős magyar internetes, az IPv4–IPv6-átmenet szakértője, az Arcok a háló mögül című könyv szerzője*

TÉVEDÉSEK VÍGJÁTÉKA – AVAGY HÁNY INTERNETHASZNÁLÓ IS VAN?

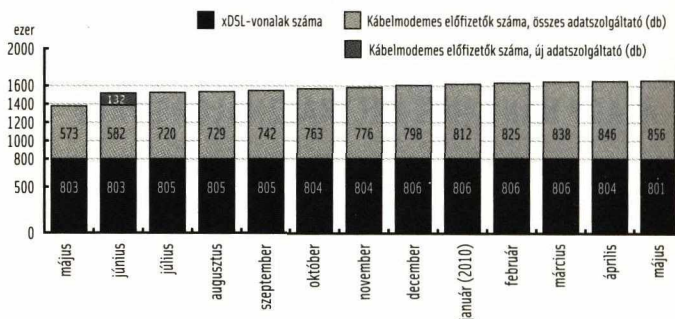
A címben szereplő *Tévedések vígjátéka* Shakespeare komédiájára utal. A cím második része lenne a kérdés: hány internethasználó is van Magyarországon? Ahány szerző, annyi válasz: a számok nagyon szórnak – vígjátéki a szituáció. A végén majd kitérünk arra is, hogy mi a veszély abban, ha ezt a kérdést nem értjük meg eléggé.

Mi sem vállaljuk, hogy megmondjuk a tutit. Már csak azért sem, mert az internet még ma is eléggé gyorsan változik. Ha pontosan tudnánk is, hogy 2009 szeptemberében hány internethasználó volt Magyarországon, akkor sem tudnánk, hogy hány internethasználó van ma.

Aztán meg az internethasználók is nagyon különböznek: aki négy órát használja a világhálót havonta, az eléggé másképp használja, mint aki negyven órát hetente. Tehát a számokat nemcsak pontosítani, hanem árnyalni is kellene. Nézzünk körül az interne-

ten, milyen használható adatokhoz férünk hozzá. Hiteles statisztikákat elsősorban a Központi Statisztikai Hivatal (www.ksh.hu) és a Nemzeti Hírközlési Hatóság (www.nhh.hu) tud szolgáltatni. Kezdjük az utóbbival.

Némi újjgyakorlat nem árt ahhoz, hogy a töménytelen információ közt megtaláljuk a bennünket érdeklőket. A keresőfelületen írjuk be, hogy „vezetékes_jelentés” (idézőjelek nélkül!), s máris megkapjuk havi bontásban a telefonvezetékes és a kábeltéves szolgáltatásokra vonatkozó statisztikákat, ideértve a vezetékes internetszolgáltatások statisztikáit is. Ezek eléggé pontos adatok, mert a szolgáltatók adataira épülnek. E cikk írásakor (2010. augusztus elején) a legfrissebb a 2010. május végi adatokat tartalmazó jelentés volt (1. grafikon).



1. grafikon. Szélessávúinternet-elérések – 2010. május

Mit látunk a 2010. májusi adatsoron? Először is azt, hogy a telefonvezetékes (xDSL) elérések száma hosszú ideje stabil, kicsivel haladja meg a 800 000-et. Másodszor azt, hogy a kábeltéves rendszerek feletti internetszolgáltatás ennél egy kicsivel több, és az utóbbi időben bővült is, most 856 000-nél tart. Harmadszor pedig azt, hogy 2009 májusa és 2009 júliusa között valami történt: hirtelen megugrott az előfizetős szám, majdnem 150 000-rel!

Ennek magyarázatát a jelentés elején találjuk meg: míg 2009 májusáig csak a nagy szolgáltatók jelentették előfizetői adataikat, 2009 júniusától már sok kisebb kábeltéves szolgáltatató is, s ez rögtön 132 000 fős ugrást eredményezett! A kis szolgáltatók ada-

taik korábban csak becsülték, s ezek a becslések nem voltak rossz-
szak, de a mért adatok most mindenképpen pontosabbak, úgy
8%-kal, ami elég jelentős különbség!

Mondhatjuk-e azt, hogy 2010 májusában összesen 1 657 000
internethasználó volt Magyarországon? Természetesen nem!!!

Elsősorban azért nem, mert egy előfizetést átlagban nem egy
ember használ, hanem kettő-három. Ha ezt figyelembe vesszük,
sokkal nagyobb számot kapunk! De az is igaz, hogy egyes háztar-
tásokban mind a kábeltelevíziós, mind a telefonvezetékes interne-
tet előfizetik, mert csomagban veszik a szolgáltatást, s ez nem ke-
rül több vagy sokkal több pénzbe. Ez az összefüggés kismértékben
csökkentheti az internethasználókra vonatkozó becslésünket.

A szélessávú vezetékesinternet-szolgáltatás mellett azonban
még mindig él a behívásos, modemes internet, még ha jelentőse-
ge ma már marginális is. Továbbá: egyre jobban terjed a mobilin-
ternet – ami viszont általában nem az egyedüli internetszolgálta-
tás, hanem kiegészíti a vezetékes szolgáltatást. E szempontok alap-
ján növelni kell az internethasználókra vonatkozó becsléseinket.

Van egy korántsem jelentéktelen felhasználói kör, amelyik csak
a munkahelyén vagy csak az oktatási intézményekben, kollégium-
okban, könyvtárakban használja az internetet. Ma a Sulinet, a Köz-
háló és az e-Magyarország programoknak köszönhetően 3-500 000
ember is lehet, aki csak így éri el, de így eléri az internetet.

A Sulinet, a Közháló, az e-Magyarország kormányprogra-
moknak köszönhető, hogy talán nincs is olyan iskola, ahonnan
nem lehet elérni az internetet, ideértve az általános iskolákat is.
Ám ez nem jelenti azt, hogy minden településen elérhető a szé-
lessávú vezetékes internet: a gazdasági racionalitás már ahhoz
sem elegendő, hogy a közepes méretű falvakban elérhető legyen,
a tanyavilágról, hegyvidékről már nem is beszélve. (Ez az egyik
oka annak is, hogy a telefonvonalra kapcsolt modemen keresz-
tüli, behívásos, keskenysávú internet még ma is használatos.)

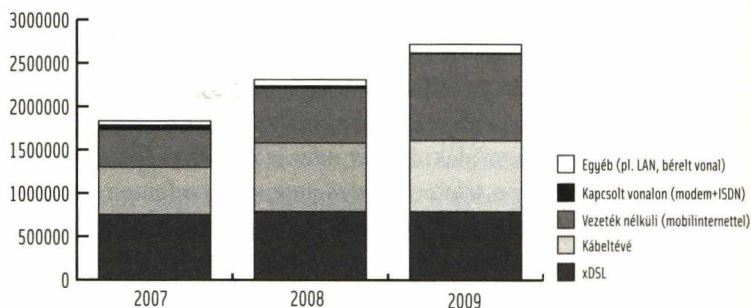
A nagyobb területen szétszórót, viszonylag kevés felhasználót
az új mobilszolgáltatásokkal lehet majd legkönnyebben, legol-
csóbban elérni.

Összefoglalva a fentieket: A szélessávú vezetékesinternet-szolgáltatások száma jól mérhető, ez a szám 2010 májusában Magyarországon elérte az 1,65 milliót. Ám azt, hogy hányan használják ezeket a hozzáféréseket, nem tudjuk. Otthoni környezetben a hivatalos becslések szerint legalább 3 millióan, de az is lehet, hogy többen, mert a többszörös használatot, a megosztás mértékét pontosan nem tudjuk megbecsülni. Ráadásul a megosztás egyik része illegális, ezért statisztikai módszerekkel is nehezen mutatható ki, mert az, aki részt vesz benne, nem beszél róla.

A következőkben arra térünk ki: mennyiben segít a statisztika ahhoz, hogy pontosítsuk az internethasználat mértékét; melyek az internet-hozzáférés illegális megosztásának veszélyei; mi az internet további elterjedésének akadályai.

Amiben a statisztika segíthet

Nézzünk körül a Központi Statisztikai Hivatal honlapján, és keressünk olyan adatokat, amelyek segíthetnek bennünket. Most másképp keresünk. Bemegyünk a letölthető kiadványok menüpont alá, itt pedig válasszuk ki a *Magyarország számokban, 2009* kiadványt.¹ Ennek 54. és 55. oldalán is találunk fontos adatokat (2. grafikon; 1. táblázat).



2. grafikon. Az internet-előfizetések száma kapcsolattípusonként (KSH)

Megnevezés	2007	2008	2009
Mobiltelefon	86,4	88,0	90,4
Asztali számítógép	50,6	54,6	56,8
Laptop	11,4	15,7	21,0
Palmtop	1,8	2,8	3,6
Internetkapcsolat	38,4	48,4	55,1
Ebből: szélessávú internetkapcsolat	33,0	42,3	50,9

1. táblázat. A háztartások ellátottsága információs és kommunikációs eszközökkel (a háztartások arányában, %)

Mielőtt a fenti adatsorokhoz észrevételeket fűznénk, keressünk még egy adatsort, ami a háztartásokra vonatkozik. Ezt az 51. oldalon találjuk meg, a táblázat elejét vesszük szemügyre (2. táblázat).

Településtípus	Lakások száma, ezer db	Száz lakásra jutó népesség, fő	Összlakosság, ezer fő, kerekítve
Budapest	890	194	1 727
Többi város	2 148	239	5 134
Községek	1 293	243	3 142
Összesen	4 331	231	10 003

2. táblázat. Lakásállomány, laksűrűség, 2009

A városokban él a lakosság 69 százaléka, községekben és tanyán 31 százaléka. A városokban van 3 millió lakás (háztartás), a községekben 1,3 millió. Az 1. és a 2. grafikon szerint 2009-ben a vezetékes szélessávúinternet-szolgáltatás elérte a 1,5, milliót, és növekedése lelassult.

Nem tudjuk viszont, hogy mekkora az átfedés a kábeltelevíziós és a telefonvezetékes szélessávú internettel ellátott háztartások között. Nem a potenciálisan elláthatók, hanem a tényleges előfizetők szerint, csak egyéni tapasztalataink alapján feltételezzük, hogy ez az átfedés nem túl nagy. Azt még kevésbé tudjuk, hogy a mobilinternet-szolgáltatást hány olyan háztartásban veszik igénybe, ahol szélessávú vezetékes szolgáltatást nem vesznek igénybe, és így a mobilinternet nemcsak egy kiegészítő szolgáltatás, hanem „az” internetszolgáltatás.

Egy lakásban Magyarországon átlagosan 2,3 fő lakik. Ha az adott lakásban valaki használja az internetet, akkor az esetek nagy részében a többiek is (gyönyörködtető, hogy 3-4 éves gyerekek hogy tudnak az internettel játszani), tehát ha az mondjuk, hogy egy otthoni szélessávú vezetékes elérés mögé átlagosan két felhasználót számolunk, akkor nagyot nem tévedünk. A felhasználók száma mindenképpen kicsit kevesebb lesz a lakosok számánál, hiszen az egészen kis gyerekek nem interneteznek, és az idősebbek egy része sem.

Az otthoni vezetékesinternet-használók száma így 3-3,3 millió lehet, tehát a magyar lakosság durván egyharmada, nem számítva a potyautasokat. Ha az lenne a helyzet, hogy a mobilinternet független lenne a vezetékes internet használatától, azaz jelentős lenne azon háztartások száma, ahol szélessávú vezetékes internetet nem, de mobilinternetet használnak, akkor a 2. grafikonon szereplő 2,5 millió előfizetői számot 2-vel szorozva kapnánk meg az 5 millió felhasználót, illetve az 50-55%-os otthoni internethasználati arányt – ezt azonban egyelőre túlzott optimizmusnak tartom. Már csak azért is, mert az 1. táblázat tanúsága szerint a háztartások 50-56%-ában van otthoni asztali számítógép, tehát közel annyi internethasználó lenne, mint ahány otthoni asztali számítógép van. Bár tudjuk, hogy internetezni lehet lap-

topról vagy okostelefonról is, ezek az eszközök leginkább olyan háztartásokba kerülnek, ahol már van asztali számítógép is.

Összefoglalva: Magyarországon a lakosság legalább egyharmada és legfeljebb fele tud otthonról internetezni.

Potyautasok és az internet-hozzáférés illegális megosztásának veszélyei

Bármennyire olcsó is ma már az otthoni előfizetés, soha nem lesz olyan olcsó, hogy ne lenne olcsóbb más előfizetését használni, akár ingyen, potyautasként, akár úgy, hogy egyeztetve kapcsolodom be a szomszédomon keresztül az internetbe, s esetleg még a költségeket is megosztjuk.

Mindkét megoldás illegális, mert az a szerződés, amelyet a szolgáltatómmal kötöttem, erre nem hatalmaz fel. Ugyanakkor mindkettőt nehéz bizonyítani, büntetni.

Potyautasok mindig voltak és mindig lesznek. Az IP alapú televíziós szolgáltatást (IPTV) nem könnyű potyautasként igénybe venni, ez tehát arra csábíthatja a potyautast, hogy váljon rendes előfizetővé. Egyébként potyázni könnyű, s a potyázás módszerei fülbesúgással is terjednek.

Otthon a legtöbb háztartásban kiépítenek egy kis helyi hálózatot, hogy több számítógép is csatlakozhasson az internethez. Mibe kerül ezt a kis hálózatot kiterjeszteni a szomszéd lakásra?

Sokan nem fáradnak azzal, hogy vezetékeket húzogassanak ki: a vezeték nélküli (általában WIFI) kapcsolatok is könnyen kiépíthetők. Ez utóbbiak védelme azonban általában kívánnivalót hagy maga után, könnyen feltörhető, vagy egyáltalán nem létezik. Azaz könnyű belépni.

Ilyen potyautas lenne a KSH statisztikáiban szereplő „mobil-internet”-használók egy része? Ha ezek a statisztikák kérdőíves felméréssel készültek, akkor nagyon is lehetséges. Személyes tapasztalatomnak sem mondana ellent, ha a potyautasok számát a szélessávú vezetékes előfizetők 10-20%-ában becsülnénk meg, ami 3–600 ezer internethasználót is jelenthet országosan!

A potyautasok nagy része semmi kárt nem okoz, ám nagyon is okozhat, akár véletlenül, akár szándékosan. Leginkább azzal, hogy olyasmit csinál, ami tilos.

Az interneten kerengő levélszemét nagy részét profi visszaélők generálják, akik potyautasként jelentkeznek be mások hálózatába, s innen kiindulva törnek fel gépeket másutt, ahonnan a levélszemétet is küldöztetik. Gondolom, senki sem örülne annak, ha a rendőrség kopogtatna az ajtaján, hogy az elmúlt napokban az ő hálózatról kiindulva töltöttek le/föl gyerekpornót, kerestek az interneten bombagyártási recepteket, küldtek fenyegető leveleket egyes minisztériumokba. S lehet, hogy mindez valóban megtörtént, csak épp egy ismeretlen potyautas tette meg. De amíg az utóbbi kiderül...

Mi az internet további elterjedésének akadályai?

Akadályból több is van: infrastruktúra-hiány; szegénység; kulturátlanság; maga az internet technológiája.

A fenti négy fő ok közül elsősorban az elsővel szoktak foglalkozni – a negyedikkel, magával az internettel viszont szinte egyáltalán nem! Pedig jobb lenne, ha minden döntéshozó értené, hogy kinőttük a jelenlegi internetet, alapos, lényeges technológiai változás előtt állunk, és amíg ezt nem lépjük meg, addig nem tudunk továbbfejlődni, hiába is lesz egyre több laptop és okostelefon!

De kezdjük az első ponttal, az infrastruktúrával.

A 2. táblázat összefoglalja a magyar lakosság lakhely szerinti eloszlását: durván 70% városokban, 30% községekben él. Sajnos az nem derül ki, hogy ezen belül hogyan oszlanak meg a községekben lakók. A városok csaknem teljes területén rendelkezésre áll vagy viszonylag olcsón kiépíthető a szélessávú vezetékes infrastruktúra, sőt részben mind a kábeltelevíziós, mind a telefonvezetékes ki is épült. 1-2 millió ember, főként községekben, tanyán viszont olyan településeken, településrészekben lakik, ahova nem építhető ki gazdaságosan vezetékes szélessávú internet. Ez tehát a magyar lakosság 10–20%-át érinti.

Ez önmagában a mobilinternet fejlesztésével sem oldható meg, mert a mobil-bázisállomás is csak azt a sávszélességet tudja szétosztani, amit odavisznek, azaz legalább a mobilelosztók második szintjéig el kell vinni az üvegszálakat.

A magyar lakosság nem kis része annyira szegény, hogy elemt napigondjai vannak. Ezt jelzi, hogy 1,3 millió BAR-listás felnőtt lakos van, azaz olyan személy, akinek a bankok nem adnak hitelt, mert több hónapon keresztül nem törlesztett időben. Ez a szám Magyarországon a hitelválságként elhíresült gazdasági válság kapcsán alakult ki 2008-tól kezdve 2009 végére. A bajba jutottak és fiatalok családtagjaik minden lemondható szolgáltatásról lemondanak, beleértve a telefont és az internetet is, már ha volt egyáltalán. Ez a szegénység jelenleg legalább 2 millió embert érint, és hatása szerencsés esetben is csak lassan fog elmúlni.

Kulturálatlanság, kulturális elutasítás

A két ok egyáltalán nem azonos. Tudjuk, hogy az oktatási rendszer a tanulók egy részét képtelen megtanítani valóban írni és olvasni: őket nevezzük funkcionális analfabétáknak. Egy funkcionális analfabéta az internetet sem fogja tudni teljesértékűen használni. Sajnos a funkcionális analfabéták száma nem csökken, a 20%-ot is meghaladja Magyarországon a 18 év feletti lakosságra vetítve.

A kulturális elutasítás részben az időskorúak körében, részben az egész ipari civilizációt is elutasító fiatalok körében is megfigyelhető. Nem kell az internet, mert az nem a mi világunk...

Az internet maga a bűnös – kinőttük a technológiát

Magyarországra közel húsz éve, 1991-től sikerült behoznunk az internetet. Mondhatnám azt is, hogy a rendszerváltás, a szövetségi rendszerváltás első kézzelfogható eredménye volt, hogy az

internethez csatlakozhattunk. Először inkább szimbolikusan, azután tömegesen is.

Az internet szabványosító-tervező szervezete, az IETF² már 1992–1993 folyamán elkezdte tervezni az újgenerációs internetet, amelyet később IPv6-nak neveztek el. Jelenleg az IPv4-et használjuk, azaz a 4-es verziót, de ezt így csak a szakma szűk rétegében hangsúlyozzák, mindenki más csak IP-ről, azaz Internet Protokollról beszél.

Az internetes kommunikáció során az egyik hálózathoz a másikba küldünk csomagokat, és hogy melyik hálózathoz melyikbe, s azon belül melyik gépnek, azt 32 bites IP-címekkel írjuk le a jelenleg elterjedt IPv4-es verzióban és 128 bittel az IPv6-osban. Már a 32 bit is úgy 4 milliárd egyedi azonosító képzésére alkalmas, ami elég nagy szám, de a leggyorsabb, legnagyobb útvonalválasztó gépek sem tudnak néhány százezernyi útvonalválasztásnál többet megjegyezni, elég gyorsan kezelni, nem is beszélve a kisebbekről. Ennek következtében is az IP-címeket csak úgy lehet kiosztani, hogy közben ne kelljen nagyon sokféle útvonalválasztást megjegyezni, karbantartani. A könnyű áttekinthetőség kedvéért az elején, az internet kezdetekor és az IP-címek kiosztásának kezdetekor nagyon kemény szabályozást vezettek be, aminek egyik következménye az lett, hogy a még kiosztható címtartomány fele már 1994-re elfogyott, pedig ekkor még csak kevesen interneteztek!

2011-ben be fog következni az, hogy már minden IPv4-es címet kiosztottak annak ellenére, hogy 1994-től kezdve nemcsak az új IPv6 protokollt tervezték meg, próbálták ki, hanem a régi IPv4-ben is bevezettünk sok-sok változtatást ahhoz, hogy tovább lehessen életben tartani.

2011-ben viszont nem a fényt fogjuk látni az alagút végén, hanem a falat: nem lehet tovább halogatni az IPv6 tömeges bevezetését.

Hol lesz a legnagyobb szükség friss IP-címekre? A szélessávú szolgáltatásokban.

Hol vagyunk legkevésbé felkészültek az IPv6 támogatásában? A szélessávú szolgáltatásokban és a tartalomszolgáltatásokban.

Az internet további elterjedésének legnagyobb akadálya maga az internettechnológia, amelyet radikálisan le kell cserélni ahhoz, hogy tovább tudjunk lépni. Be kell vezetni az IPv6-ot.

Ezt a cserét néhányan szerették volna a felhasználók bevonása nélkül megtenni, de ma már tudjuk, hogy ez lehetetlen. Mozgalmat kell szervezni. Együtt működünk.

JEGYZETEK

TALYIGÁS JUDIT: Felvezetés

1 2008. február 27-én az Európai Bizottság új, biztonságosabb internet-programra nyújtott be javaslatot, amelynek célja a gyermekek online környezetben belüli védelmének erősítése. Az új program, amelyet az Európai Parlament 2008. október 22-én elfogadott, a web 2.0 legújabb kommunikációs szolgáltatásait (például a társasági hálózatokat) is felöleli, s nemcsak a jogellenes tartalmak ellen veszi fel a harcot, hanem az olyan káros viselkedésformák ellen is, mint a zaklatás vagy a bizalmaskodás. Előzménye az 1999-ben indított Biztonságosabb Internet Akcióterv, majd a 2004-ben indított Safer Internet Plus program. A jelenlegi, 2009-től 2013-ig tartó program 55 millió eurós költségvetéssel rendelkezik.

2 A Neumann János Számítógép-tudományi Társaság konferenciája, Budapest, 2009. május 26.: „...a kockázatokról és mellékhatásokról kérdezze meg...” (Az internethasználat pszichológiai és társadalmi haszna és veszélyei). Lásd még <http://de.njszt.hu/rendezvenyek/ihpthv>

3 Ez az egyedülálló, többnyelvű rendszer médiaforrásokból – például hírekből, blogokról és weboldalakról – gyűjti és terjeszti a vonatkozó információt a betegségek kitöréséről és a közegészségügyi eseményekről.

4 http://www.police.hu/nyitooldal/cikkek/orf100705_01.html

CSEPELI GYÖRGY: Veszélyesen élni? Avagy az internethasználat kockázatai

- 1 Hankiss Elemér (1928–) magyar szociológus, filozófus, számos külföldi egyetem vendégprofesszora.
- 2 Ulrich Beck (1944–) német szociológus, a müncheni és a londoni egyetem professzora.
- 3 Niall Ferguson (1964–) az Egyesült Államokban élő, a Harvardon tanító brit történész.
- 4 Adam Smith (1723–1790) skót klasszikus közgazdász és filozófus. Általában őt tartják a modern közgazdaság-tudomány atyjának.
- 5 Voltaire *Candide vagy az optimizmus* című művében a bölcs Pangloss mester szerint minden a legjobban van ezen a legeslegjobb világon.
- 6 Kémprogramnak (*spyware*) nevezik az olyan, interneten terjedő számítógépes programokat, amelyek célja, hogy törvénytelen úton megszerezzék a fertőzött számítógép felhasználójának személyes adatait.
- 7 Jelszólopáshoz a billentyűzet lenyomását naplózó programokat használnak.
- 8 Speciális program települ a gépre, mely a háttérben fut anélkül, hogy a számítógép gazdája azt észrevenné. Ezzel a botnet hálózat részévé teszi. A botnet célja, hogy nagy teljesítményű, gyors, mégis anonim infrastruktúrát nyújtson a spammernek, amellyel az könnyen és gyorsan tud nagy mennyiségű spamet küldeni, illetve más törvénytelen cselekedeteket folytatni. A modern vírusvédelmek felismerik az ilyen típusú programokat, azonban nagyon sokan nem vagy elavult vírusvédelmet használnak.
- 9 A felhasználó a saját számítógépéről egy tőle – általában fizikailag is – távol lévő számítógépen futtat le programot, amelyről esetleg adatok, eredmények érkeznek a saját gépére.
- 10 Carl Friedrich Gauss (1777–1855) német matematikus és természettudós. A tudományok számos területének fejlődéséhez járult hozzá, így a számelmülethez, az analízishez, a differenciálgeometriához, a geodéziához, a mágnesességhez, az asztronómiához és az optikához. Gauss a „matematika fejedelmé”-nek is nevezik. – A statisztikában a legfontosabb és leggyakrabban alkalmazott eloszlás a normális eloszlás. A normális eloszlás jellegzetes haranggörbéjét egy francia matematikus, Abraham de Moivre fedezte fel és közölte 1733-ban. Tudományosan két matematikus-csil-

lagász, a francia Pierre-Simon Laplace és Gauss alapozta meg. Gauss után nevezték el a normális eloszlást Gauss-eloszlásnak, mivel Gauss volt az első, aki a normális eloszlást az égitestek mozgására alkalmazta.

11 A szerző a Gauss-görbénél a megismerés mértékét a függőleges, míg a megismerők számát a vízszintes koordinátára vonatkoztatja, és így a jellegzetes haranggörbe esetében jól érzékelhető, hogy csak kevesen érnek el kiemelkedő megismerést, tudást.

12 Everett M. Rogers (1931–2004) szociológus elsősorban az innováció kérdéseivel foglalkozott.

13 Az iparágat előrehajtó, élenjáró technológiai megoldásokkal rendelkező, új alkalmazás, amelyre az igazán érdeklődő felhasználók azonnal felfigyelnek. Így a *killer application* szükséges, sőt igen fontos eleme az informatikai iparnak. Gyilkos hatással van a piaci vetélytársakra, vélhetően innen a kifejezés.

14 Bard és Söderquist *Netocracy* című könyve alapján: a versenyben kiszoruló új osztály, a netokrácia tagjai a Föld bármely pontjáról származhatnak; nincs polisz, melynek javáért küzdeni akarnának, egyedül önmagukért harcolnak. A netokrácia az információt birtokló, kezelő, szűrő új osztály.

15 Médiapolgár; a szó, amely maga is utal erre, az internetes tartalmakat is generáló, amatőr felhasználót jelenti.

16 A *digitális bennszülött* és *digitális bevándorló* fogalmakat Marc Prensky használta 2001-ben megjelent „Digital Natives, Digital Immigrants” című, kétrészes cikkében. A cikkben Prensky kifejti, hogy környezetünk – különös tekintettel az új infokommunikációs lehetőségekre (számítógépes hálózatok, mobiltelefon) – hogyan változtatja meg a gyermekek oktatással szemben támasztott igényeit. Bevezeti a *digitális bennszülött* (gyermek) és a *digitális bevándorló* (tanár) fogalmát. Digitális bevándorlók (*digital immigrants*) mindazok, akik felnőttként tanulták meg az információs környezetben való tájékozódáshoz szükséges ismereteket. Digitális bennszülöttek (*digital natives*) azok a korosztályok, amelyek tagjai gyermekként, szocializációjuk legérzékenyebb szakaszában, természetes környezeti adottságként váltak információsán írástudóvá. Felhívja a figyelmet arra, hogy a tanároknak és az oktatásnak kell igazodniuk a megváltozott tanulói elvárásokhoz. Az újfajta megközelítést, a „jövő” oktatási tartalmát példákön keresztül mutatja be.

17 Gulácsy Lajos (1882–1932) festő képzeletbeli országa.

18 Alan Turing 1950-ben vetette fel a Turing-teszt koncepcióját, amely arra hivatott, hogy az adott gépezetről megállapítsa, képes-e gondolkodásra. A teszt lényegében abból áll, hogy az ember pusztán billentyűzet és monitor közvetítésével kérdéseket tesz fel a két tesztalanynak, akiket így se nem láthat, se nem hallhat. A két alany egyike ember, míg a másik gép – mindketten megpróbálják meggyőzni a kérdezőt arról, hogy ők gondolkodó emberek. Ha a kérdező hosszas faggatás után sem tudja teljesen egyértelműen megállapítani, hogy a két alany közül melyik az ember, akkor a gép sikerrel teljesítette a tesztet.

19 Valamely lázas betegségnek, de különösen elmebetegségnek hirtelen kitörése.

20 Angol politikai irányzat, amely az elszigetelődést hirdette.

21 A géprombolók mozgalma.

22 Elmosódott határú halmazok logikája.

23 A *Népszabadság* újságírója, akinek cikkeiben a szerző az információs társadalom lejárását és kriminalizálását látta.

SZABÓ ENDRE GYŐZŐ: A személyes adatok védelmének kérdései a virtuális világban

1 A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló, 1992. évi LXIII. törvény így definiálja a személyes adatot: bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetve egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

2 A magyar gyakorlat a szerződések megkötésekor általában a természetes személyazonosító adatok megadását írja elő. A név, születési hely, idő és az anya neve tartozik hagyományosan a természetes személyazonosító

adatok körébe. A szerződések kötésekor ezt az adatkört rendszerint kiegészítik a laccímmel, továbbá annak az okmányoknak a számával, amelyben az adatok szerepelnek.

3 Az adatvédelmi jog az élő természetes személlyel összefüggésbe hozható adatokat tekinti személyes adatoknak. Az olyan adatokat, amelyek elválaszthatatlanul kötődnek két vagy több személyhez, közös adatoknak nevezzük. Ilyen lehet például egy fénykép, amelyen többen is láthatók. A közös adatok kezeléséből adódó problémákra e tanulmány keretében nem térünk ki.

4 Különleges adat az 1992. évi LXIII. törvény 2. § szerint

- a) a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselési szervezeti tagságra,
- b) az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat.

5 Bár hosszas vita előzte meg a döntést, a kézirat lezárásakor ismert információk szerint a 2011-es népszámlálás során használt kérdőíven – a hagyományoktól eltérően – nem fog szerepelni a felekezeti hovatartozásra vonatkozó kérdés.

6 A Legfelsőbb Bíróság 14. számú polgári kollégiumi állásfoglalása szerint nincs helye sajtó-helyreigazításnak, ha a sajtószerv valamely büntető eljárás jogerős befejezése előtt a valóságnak megfelelően tájékoztatta olvasóit a vádirat tartalmáról, a nyilvános tárgyalásról, vagy a nem jogerős bírósági ítéletről. Ha a büntetőeljárás nem vezet elmarasztalásra, a sajtószerv az érintett személy kérelmére köteles az olvasókat erről is – díjtalanul – tudósítani.

7 A célhoz kötött adatkezelés követelményét fogalmazza meg a konkrét esetre a Munka Törvénykönyve: 77. § (1) A munkavállalótól csak olyan nyilatkozat megtétele vagy adatlap kitöltése kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely személyiségi jogait nem sérti, és a munkaviszony létesítése szempontjából lényeges tájékoztatást nyújthat. (2) Tilos a munkavállalót terhesség megállapítására irányuló vizsgálat elvégzésére, illetve erről szóló igazolás bemutatására kötelezni, kivéve, ha erre a munkaköri alkalmasság vizsgálata és véleményezése közben jogszabály előírása alapján kerül sor.

8 A személyes adatok felhasználásának nincs általános tilalma, általános követelményei azonban léteznek. Ha a felhasználókhöz köthető információk felhasználása a cél, akkor az adatvédelmi jog két alapvető követelményt támaszt: az első az, hogy a személyes adatok kezelése legyen mindenki számára átlátható, a másik pedig az, hogy az érintett akarata és tudta ellenére ne válhasson ilyen adatkezelések alanyává.

9 Az adatbányászat a nagy mennyiségű adatban rejlő információk félautomatikus feltárása mesterségesintelligencia-algoritmusok alkalmazásával. Széles körben elterjedt például társadalmi viselkedések vizsgálatok, de a gyógyszeripar, vegyipar területén is.

10 Az Európai Parlament és az Európa Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról.

11 A Német Szövetségi Alkotmánybíróság 2010. március 2-án meghozott ítélete, lásd http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html

12 http://ec.europa.eu/information_society/eyouguid/index_en.htm

RÁCZ BENCZE: We watch you watch

1 Külön köszönet Bencsáth Boldizsárnak, aki a Budapesti Műszaki és Gazdaságtudományi Egyetem Crysys laboratóriumából sok segítséget adott e tanulmány megírásakor.

2 Az elektronikus dokumentumhoz azonosítás céljából végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt elektronikus adat, illetve dokumentum. Ez alkalmas az aláíró azonosítására, és biztosítja az aláírt dokumentum megmásíthatatlanságát. Elektronikus aláírás bármilyen digitalizált dokumentum esetén – szöveg, film, hang – megvalósítható. 2001-ben fogadták el az elektronikus aláírásról szóló törvényt Magyarországon.

3 A szimmetrikus kulcs esetén a kódolás és dekódolás ugyanazon kulccsal történik. Maga az eljárás sokak számára hozzáférhető, csak a kulcs titkos. Ez egy adott n tagú közösség esetén, ha mindenki mindenkivel titkosan

akar adatot cserélni, nagyszámú, $(n*(n-1)/2)$ kulcsot tesz szükségessé. Ennél jobban kezelhető az asszimetrikus kulcsok rendszere, ahol mindenkinek két kulcsa van, az egyik a magán (privát), amelyet titkosan kezel, a másik a nyilvános (publikus). Ha valakinek titkosítva akarunk egy üzenetet küldeni, akkor az ő nyilvános kulcsával kódolva csak ő tudja majd magánkulcsával elolvasni, így az mások számára titkos marad.

4 Request for Comments, szó szerint: „Szóljanak hozzá!”, „Kérjük az észrevételeket!” Így nevezik az Internet Engineering Task Force, azaz az internet szabványosító szervezetének szabványait, összefoglalóit.

5 CISM – certified information security manager (minősített információbiztonsági vezető); CISA – certified information systems auditor (minősített információsrendszer-auditor);

6 CEH – certified ethical hacker (szakmai szervezet által minősített etikus hacker).

7 Publikus interneten hozzáférhető, legnépszerűbb azonnali üzenetküldő szolgáltatások.

8 A vállalat piaci értékének és könyv szerinti értékének különbsége, pl. jó hírnév, piaci értéket jelentő elfogadott márkanev.

9 A potenciális támadás erejét kifejező szleng kifejezés, amelyet a hackerek egymás között használnak elosztott szolgáltatásmegtagadásos támadásra (DDoS, lásd még a 12. jegyzetben) alkalmas hálózatot fenntartó hackerre vagy hackercsoportra.

10 Az első és a mai napig legjelentősebb kereskedelmi portálok.

11 Az az időmennyiség, amíg az áldozat szerverei nem elérhetők.

12 Egy informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérése (Denial of Service, rövidítve: DoS) történhet megosztva is, több forrásból – ekkor a támadás szokásos rövidítése DDoS (Distributed Denial of Service). A DDoS a támadások egy összetettebb fajtája, amely a támadón és a támadotton kívüli számítógépekben rejlő „erőt”, illetve a külső számítógépek nagy mennyiségét hasznosítja a támadáshoz.

13 Az 1947-ben emelt Bronzkatona más-más emlékeket idéz az oroszokban és az észtekben: míg az előbbieket a nácik ellen harcoló szovjet katonák iránti tisztelet szimbólumaként értelmezik, addig az észti lakosságot a szovjet rezsim alatti szenvedésekre emlékezteti.

14 Lásd Csepeli Györgynél a 8. jegyzetet.

15 Olyan, többnyire egyszerű programok, amelyek mindenki számára elérhetők az interneten.

16 A támadók elárasztják az áldozatot pl. egyszerű levelekkel, így annak a sávszélessége használhatatlan lesz.

17 Community Emergency Response Team – számítógép-hálózati katasztrófákat elhárító csoport.

18 Kurt Gödel (1906–1978) világhírű osztrák Einstein-díjas matematikus, logikus, tudományfilozófus.

SZÉKELY IVÁN: Kukkoló társadalom

– avagy van-e még függöny virtuális ablakunkon?

1 Aldous Huxley, *Szép új világ* (1932, negatív utópia) – a 26. századi Londonban játszódó történetben az emberiség gondtalan, egészséges és technológiailag fejlett. Nincsenek többé háborúk és szegénység, mindenki folyamatosan boldog. Elveszítették a családot, a kulturális sokszínűséget, a művészeteket, az irodalmat, a tudományt, a vallást és a filozófiát.

2 George Orwell, *1984* (1949, satirikus politikai regény és szerelmi történet). A felügyelő állam tökéletes alkalmazkodást diktál a polgárok között, hazugságokkal, félelemkeltéssel és kegyetlen büntetésekkel.

3 *The Right to Privacy*. A tanulmány, amely a privacy-irodalom kiindulópontja, több mint egy évszázaddal megjelenése után végre magyarul is hozzáférhetővé vált: „A magánszférához való jog” címmel megjelent az *Információs Társadalom* 2005. évi 2. számában.

4 III/III a magyarországi titkosszolgálat; a Ministerium für Staatssicherheit (Állambiztonsági Minisztérium), más néven Stasi Kelet-Németország politikai titkosszolgálat; a KGB (Komitet Goszudarsztvennoj Bezopasznosztyi) a szovjet Állambiztonsági Bizottság. Elsősorban titkosszolgálati részlegek, a határőrség és a kormányőrség tartoztak hozzájuk, valamint közel 300 ezer főnyi létszámú reguláris csapatok is.

5 Legújabban már a nem kívánt besorolás és sztereotipizálás elleni jogot is ide számítják, lásd Benjamin Goold cikkét.

6 Az adatvédelem (a személyes adatok védelme) csak egy szelete a privacy védelmének, de még az információs privacy védelmének is – ráadá-

sul nem is „az adatok védelméről” van szó: az legfeljebb egy technikai eszköz arra, hogy az adatok alanyait védjük, még inkább arra, hogy gyakorolhassák önrendelkezésüket adataik sorsa felett.

7 A Habeas Corpus (szó szerint: Tiéd a tested) a XVII. századi Angliában született törvény és jogelv, mely szerint senkit sem szabad törvénytelenül fogságban tartani bírói ítélet nélkül; kiterjesztett értelmezésében az ember fizikai valójával való saját rendelkezésének joga. A Habeas Data (Tiéd az adatod) ennek mintájára az ember saját adataival, kiterjesztett értelemben virtuális valójával való rendelkezésének jogelve.

8 A privacy védelmének nemzetközi évkönyve 2006-ban 75 ország törvényeit és gyakorlatát elemezte.

9 Igen tanulságos, hogy az amerikai bíróságok több mint fél évszázadig nem tudtak mit kezdeni az új jelenséggel: ítéleteikben a szilárd falat tekintették a magánélet határának, ha ezen belülre került a poloska, akkor megsértette a privacyt, ha kívülről történt a lehallgatás, akkor nem.

10 http://www.broad-project.eu/upload/Tudta_e.pdf – Az idézet forrása a *Broadening the Range of Awareness in Data Protection* (BROAD), egy holland és magyar szervezetek részvételével zajló projekt, amelynek három fő akcióterülete az informatikusok véleményének feltárása a személyes adatok kezeléséről (lásd alább), egy többnyelvű internetes fórum létrehozása a privacy és az információs technológiák metszetében, valamint kreatív alkotások létrejöttének elősegítése az adatvédelmi tudatosság növelése érdekében. (Az eddig elkészült filmek szabadon letölthetők a <http://petportal.eu/video> címről.)

11 Jeremy Bentham (1748–1832) angol jogtudós, filozófus, a hasznosságot és az érdeket az élet és az életvitel alapelvevé tevő etikai irányzat megalkotója (utilitarizmus).

12 Bentham (1787) első kéziratos vázlata ma a British Libraryben látható.

13 Michel Foucault (1926–1984) francia történész, filozófus; elsősorban a különböző társadalmi intézmények (a pszichiátria, az orvostudomány és a börtön), valamint a szexualitás történetéről szóló újszerű kutatásairól ismert. A hatalom problémáját, illetve a tudás és a hatalom viszonyát, valamint a diskurzus működését középpontba állító megközelítése számos kortárs társadalomtudományi elméletbe beépült.

14 Pedig már megszületett az internet és a web 2.0 világ kritikai politikai gazdaságtana is, lásd például Christian Fuchs munkásságát.

15 A Bush elnök által aláírt 2003-as amerikai spamtörvény megszületésében már a választópolgárok elégedetlensége is közrejátszott. A törvény voltaképpen legalizálta a spamek küldését bizonyos feltételek betartásával, aminek eredményeképpen a spamek száma megsokszorozódott, és ma már az elektronikus levélforgalom döntő többségét – egyes források szerint 97%-át – a spamek teszik ki (lásd például: http://index.hu/tech/blog/2008/10/08/hatastalan_a_spamellenes_torveny).

16 Lásd például Clive Norris brit szociológus elemzéseit.

17 Az új büntetőtan és az aktuárius igazságtétel elméletének klasszikus forrása Feeley és Simon tanulmánya.

18 *Broadening the Range of Awareness in Data Protection* (az adatvédelmi tudatosság szélesítése): www.broad-project.eu – lásd még a 10. jegyzetet.

19 Az adatvédelem biztonságát fokozó technológiák – ez egy általános fogalom, amely összefogja az online szolgáltatások (internet) felhasználói magánéletre, személyazonosításra használható adatainak védelmét szolgáló eszközöket, eljárásokat.

20 A nym-generátorok *nym*eket, vagyis *pseudonym*eket (digitális fedőneveket) generálnak; a profilgátlók igyekeznek korlátozni a felhasználói profilok felépíthetőségét; az anonim remailerek nemcsak az elektronikus levelek tartalmát, hanem a kommunikáló felek kilétét is elrejtik az illetéktelen megfigyelők elől; a cookie-irtók a *cookie*-kat (magyarul „sütitet”), vagyis a böngészési szokásaink követésére is alkalmas kis szövegfájlokat távolítják el számítógépünkről; az anonim digitális pénzrendszerek a készpénzhasználat anonimitását állítják vissza az elektronikus kereskedelembe; a spyware-irtók a tudtunk és beleegyezésünk nélkül a számítógépünkre telepített kémprogramok törlését végzik; a *bioscrypt* (bioszkript) a felhasználók önrendelkezését elősegítő, biometrikus rejtjelezést alkalmazó technológia. Az RFID-technológia elsősorban tárgyak azonosítására szolgáló, rádióhullámokkal aktiválható és visszajelző chippek alkalmazását jelenti, használata már emberek azonosítására is előfordult. – A téma színvonalas hazai fóruma a PET Portál és Blog, <http://pet-portal.eu>.

21 Lásd az Eurobarometer vonatkozó vizsgálatait, például Flash Eurobarometer 225 (2008).

- 22 Például az EPIC (Electronic Privacy Information Center), a Privacy International, vagy a magyarországi TASZ (Társaság a Szabadságjogokért).
- 23 A *surveillance* eredeti értelmében felülről figyelést, a *sousveillance* alulról figyelést jelent.
- 24 Ennek az elképzelésnek az egyik vezéralakja a Torontói Egyetem tanára, Steve Mann, aki a testére szerelt kamerával „figyeli vissza” a környezetét (Mann, Nolan és Wellman, 2003).
- 25 Ismert személyiség például Julia Scher, aki az 1980-as évek vége óta foglalkozik a megfigyelés művészi ábrázolásával, installációk és performanszok formájában. Számos alternatív filmes készít megfigyelésselles filmeket, köztük sajátos csoportot képviselnek a CCTV filmkészítők, akik kizárólag a megfigyelőkamerák képeit használják fel. Szakmai szabályaikat kiáltvány tartalmazza.
- 26 A filmek szabadon letölthetők a <http://pet-portal.eu/video> oldalról és Creative Commons licenc alatt szabadon felhasználhatóak bármilyen non-profit célra. Lásd még a 10. jegyzetet.
- 27 A Virginiai Egyetem és a George Mason Egyetem kutatói által javasolt új metafora a közösségi hálózatok megfigyelési gyakorlatának érzékeltetésére.
- 28 Ez a mottó ma aktuálisabb, mint valaha – lásd a szerzőnek a *Magyar Távközlés VII*(1996)/4. számában megjelent tanulmányát: Az adatvédelmi biztos első fél éve.

DEMETROVICS ZSOLT–KORONCZAI BEATRIX:

Az internetfüggőség néhány pszichológiai vonatkozása

- 1 Kimberly Young, Indiana University of Pennsylvania, Psy.D. Behavioral Medicine and Neuropsychology. *Caught in the Net: How to recognize the signs of Internet addiction – and a winning strategy for recovery*, New York, Wiley, 1998
- 2 Az alkalmazkodást nehezítő viselkedés, azaz olyan viselkedés, amely károsítja a személynek a mindennapi tevékenységekben való megfelelését, azt, hogy eleget tegyen a szociális szerepeiből fakadó elvárásoknak.
- 3 E zavarok közé azok a betegségek tartoznak, ahol a központi tünet az, hogy a személy nem tud ellenállni, nem tud kontrollálni valamilyen kész-

tetést (impulzust). Ide tartozik például a szerencsejáték-szenvedély, de a kleptománia vagy a pirománia is.

4 Szakorvosi felügyelet mellett szedhető gyógyszer.

Z. KARVALICS LÁSZLÓ: Az univerzális kvantor rémuralma

– avagy a veszélydiskurzusok logikai szerkezetéről

1 *Torrent*: az illegális tartalommegosztó oldalak gyűjtőneve.

2 Arról most ne essék szó, hogy a Google-nak valójában semmi köze a torrentoldalakhoz, sem a kalózkodáshoz. Matyi Dezső víziója, miszerint a Google maga a net, egyszerű (de fájdalmas) ismerethiányból fakad.

3 A „mély web” (*deep web*) az interneten tárolt olyan tartalmakat (különböző adatbázisokat, nem szöveges dokumentumokat) megnevező gyűjtőszó, amely a keresők számára a legtöbb esetben elérhetetlen, nehezen feltérképezhető, csak igen kivételesen megtalálható óriási adattömeget kívánja szemléletes formában megragadni.

4 A Wikipédia szerint 1982-ben Scott E. Fahlman, a Carnegie Mellon Egyetem professzora volt az első, aki a kettőspont, a kötőjel és a zárójel segítségével a világon először horizontális vigyorgó fejet írt egy levélben. Először főként komolytalan dolgok jelölésére alkalmazta, ami eleinte csak a számítástechnikához értő személyek körében, majd az egész világon elterjedt, hiszen az online beszélgetések során remekül pótolta az arckifejezéseket, gesztusokat. Összefoglaló elnevezésük az emóció és az ikon összevonásával képzett *emotikon*, de elterjedt a mosolygásra utaló *smiley*-nyelv elnevezés is.

5 *Cyber-bullying*: számítógépes, internetes, mobiltelefonos zaklatás.

6 A *hoax* angol eredetű vándorszó. Leginkább „beugratás”, „megtévesztés”, „átverés”, „álhír” vagy „kacsa” jelentésben az e-mailben terjedő álhírek, lánclevelek különféle változatait jelöli. Az ügyesen megkomponált hamis tartalmakat olykor az írott sajtó vagy a televízió is átveszi.

7 Amikor a második világháborús béketárgyalásokon a lengyelek kártérítést követeltek a Magyarországon átengedett csapataik elvesztett hadfelszerelésére hivatkozva, méltán írhatta Illyés Gyula: „Mérj csak egy csapással többet a bűnösre, mint amit megérdemel, s azonnal az ártatlan visszénye ragyogja be.”

8 George Orwell (1903–1950) angol író, kritikus, újságíró.

9 Negatív jövőképek.

10 Terminal.hu Online Napi Informatikai és Gazdasági Hírportál.

11 Susan Adele Greenfield, brit tudós, író, rádióelőadó, a Lincoln College (Oxfordi Egyetem) szinaptikus gyógyszeresztani professzora, a Royal Institution igazgatója. 2006. február 1-jén az edinburgh-i Heriot-Watt Egyetem kancellárjának nevezték ki.

12 Érdekes epilógus, hogy Greenfield úgy véli: a számítógép-használat tiltása nem jelentene megoldást. Ez a látszatra óvatos állítás is azt implikálja, hogy olyan horderejű veszélyt sikerült feltárni (egyébként a brit politikai elit számára), hogy legalább a megfontolás erejéig mérlegelni lehet a betiltást mint gyógymódot.

13 Rejtő Jenő (született Reich Jenő, írói álnevei: P. Howard, Gibson Lavery) (1905–1943) magyar író. Látszatra ponyvaregényeket írt, azonban életművét manapság már az irodalmi körök is nagyra értékelik.

14 Nicholas Negroponte (1943–) mérnök, a Massachusetts Institute of Technology's Media Lab munkatársa, a magyarul is kiadott (Budapest, Typotex, 2008) *Digitális létezés* című könyv szerzője 1997-ben azt jósolta, hogy az internet és a digitális technológia hatására leomlanak majd a határok a nemzetek között, és a világbéke új, édes korszaka köszönt ránk.

15 Arról nem is beszélve, hogy Negroponte azokról a fiatalokról beszélt, akikre „húsz év múlva” már igaz lehet mindez. És Morozov nem azért csal, mert nem várta meg 2017-et (világbéke akkor sem lesz), hanem azért, mert a „jóslat” nem jövőkutatói pontossággal, hanem a trend megjelölésével operált: a „húsz év” annyit jelöl, hogy nem azonnal, de nem is az iszonyú távoli jövőben.

16 1994-ben Esther Dyson és Alvin Toffler vezetésével, George Gilder és dr. George Keyworth közreműködésével megjelent a szerény címet viselő *Magna Charta* a tudás korszakához című tanulmány (The Progress and Freedom Foundation, 1994). A vízió egyik eleme szerint az amerikai eszme – köznapian szólva az amerikai álom – valósul majd meg a kibertérben is, amikor a digitális szomszédok nem földrajzi helyük, hanem közös érdeklődésük alapján kötnek szövetséget.

17 A szerzők itt a hagyományos, földrajzi közelségen alapuló közösségképződésre „ránövő”, a közös érdeklődésen alapuló új közösségi logikára gondolnak.

18 Elolvassák, és formálja a gondolkodást, közvetlenül vagy közvetve befolyásolja a szellemi útvalasztásokat, de nem épül be saját közleménybe. Részében vagy egészében szakirodalommá válik felsőoktatási intézményben, és nagyon sokan szereznek ebből ismereteket. De még az is hasznosulás, amivel egy adott rendszerezés hozzájárul a szerző gondolkodói fejlődésének valamelyik állomásához.

19 A *pocket monster* – magyarul zsebszörny – kifejezés elemeiből összekombinált mozaikszó.

20 Ennek sokszor „megénekelte”, ismert tantörténete a cseh Sulinet öskorában játszódtott. A döntéshozók szilárd vélekedése volt a számukra „tálatl” adatok alapján, hogy a diákok csakis mihaszna tevékenységeket folytatnak az interneten, elsősorban online szexoldalakat keresnek, így legfontosabb feladatuknak azt tekintették, hogy drága és hatalmas tűzfalakkal megóvják a felnövekvő generációt a kártékony tartalmaktól.

21 Régebbi és frissebb keletű példákra lásd http://index.hu/tech/2009/05/08/felelem_es_retteges_a_webkettotol/

22 Z. Karvalics László, Hajrá, digitális bennszülöttek!, *Szitakötő*, 2009/1, Tavasz, 2–3.

23 A fogalmak értelmezéséhez lásd Csepeli Györgynél a 16. jegyzetet.

TALYIGÁS ANIKÓ: Az informatikaoktatás dinamikája

1 Külön köszönet Dancsó Tündének a munkámhoz nyújtott segítségért.

2 European Computer Driving Licence, Európai Számítógép-használói Jogosítvány – az Európai Unió által támogatott, egységes európai számítógép-használói bizonyítvány, amely az informatikai felhasználói ismereteket, az informatikai írástudás meglétét hivatott igazolni.

3 Lásd Talyigás Juditnál a 2. jegyzetet.

VAJDA ZSUZSANNA: A gyerekek és a számítógép

1 Seymour Papert (Pretoria, Dél-Afrika, 1928. március 1.) matematikus az MIT-n, számítógéptudós, pszichológus, kiváló pedagógus. A mesterséges

intelligencia úttörőinek és a LOGO programozási nyelv megalkotóinak egyike.

2 2004-ben az Informatikai Minisztérium kezdeményezésére kísérletképpen több óvodában is telepítettek számítógépet, és használatukra az óvónőket is kiképezték.

3 Lásd például Hírextra, 2010. június 15.

4 Olyan fakultatív tantárgy bevezetését tervezik – a pedagógusok előzetes felkészítése után –, amely a szexualitás és ezen belül a pornográfia kérdéseit is érinti – a felvilágosítás, a megbeszélés érdekében. A megkérdezett hazai iskolaigazgatók más-más okból, de ezt elutasítják. (A szerk. megjegyzése)

SZABÓ GYÖRGY: Virtuális világ és valós tér. Utópiák, realitás, veszélyek

1 Atlasz a görög mitológiában a titánok leszármazottja, az óriás, aki a válán tartja az égboltot.

2 Johann Heinrich Lambert (1728–1777) svájci matematikus, fizikus és csillagász.

3 Louis-Jacques-Mandé Daguerre (1787–1851) francia vegyész, a fényképezés történetének egyik úttörője. Az a probléma foglalkoztatta, hogy milyen technikai eszközzel lehetne létrehozni a világ képmását. 1839-ben hozta nyilvánosságra az 1837-re kifejlesztett és róla elnevezett dagerrotípiát.

4 Gaspard Felix Tournachon (1820–1910) francia író és karikaturista. A légi fotózást elsőként gyakorolta Párizsban, 1858-ban.

5 GPS, GSM, WIFI, RFID.

6 Alapelve a hálózat bázisállomásai (nagyobb hatótávolságú GSM, kisebb hatótávolságú RFID, WIFI antenna pozíciója) és a mobil egység (mobiltelefon, RFID-tag, WIFI-képes mobil eszköz) közötti elektromágneses jel terjedési idejének, utazási távolságának, irányának alapján a geodézia pontmeghatározási módszereivel (hátrametszés, előmetszés) a mobil egység pozíciójának kiszámítása. A cellaazonosító alapú (Cell-ID) megoldás szolgáltatja a mobil egységet tartalmazó cella azonosítóját. A geodéziai előmetszést megvalósító AOA (Angle of Arrival) megoldás és a távolságmérésre visszavezethető TOA (Time of Arrival), TDOA (Time Difference of

Arrival) és E-OTD (Enhanced- Observed Time Difference) módszerek alkalmazásának nehézsége abban rejlik, hogy a hálózat komponenseit és szoftverkörnyezetét a kommunikációs funkciók mellett a helymeghatározási funkciókra is fel kell készíteni. A mobil eszköz alapú (GPS) és a hálózati technológiák (GSM) előnyeinek integrálását kísérelik meg a hibrid pozicionáló rendszerek. Az A-GPS (Assisted-GPS) megoldás egyesíti a GPS nagyobb kültéri helyzeti pontosságát és a fedett városi, beltéri területeken a GSM rendelkezésre állási biztonságát, 10 m alatti helyzeti megbízhatóságot eredményezve.

7 Theodore Roszak, *Az információ kultusza, avagy a számítógépek folklorja és a gondolkodás igaz művészete*. (ford.: Geigler Györgyi) Budapest, Európa Kiadó, 1990, 304. o.

TURCHÁNYI GÉZA: Tévedések vígjátéka – avagy hány internethasználó is van?

1 <http://portal.ksh.hu/pls/ksh/docs/hun/xftp/idoszaki/mosz/mosz09.pdf>

2 Internet Engineering Task Force, nemzetközi szakmai civilszervezet az internet szabványosítására, lásd még Rácz Bencénél a 4. jegyzetet.

A SZERZŐKRŐL

Csepeli György

Szociálpszichológus, az ELTE egyetemi tanára. Kutatási területe a társadalmi identitás, a csoportközi viszonyok szociálpszichológiája. Kutatásai a nemzeti érzés- és tudatvilág, az előítéletek és sztereotípiák szerveződésének és működésének szociológiai, szociálpszichológiai meghatározóinak feltárására irányulnak. Kutatási területe néhány éve kiegészült az új infokommunikációs technológiák társadalmi és lélektani hatásainak vizsgálatával, melynek keretében a hálózatosodás és a társadalmi egyenlőtlenségek közötti kapcsolatot, az új kommunikációs architektúra és a kultúra közötti viszonyt vizsgálja. Legújabban az új tekintélyelvűség jelenségvilágát elemzi, melynek megnyilvánulásai elválaszthatatlanok az új infokommunikációs technológiák adta lehetőségektől.

Demetrovics Zsolt

Klinikai addiktológiai szakpszichológus, kulturális antropológus, PhD-fokozatot addiktológia tárgykörben szerzett az ELTÉ-n. Az ELTE Addiktológiai Tanszéki Szakcsoportjának vezetője, a Nemzeti Drogmegelőzési Intézet tudományos munkatársa. Főbb ku-

tatási területei: a szenvedélybetegségek epidemiológiája, különös tekintettel a rekreációs színtéren megjelenő droghasználatra és a viselkedési addikciókra; a droghasználat személyiségpszichológiai és családindinamikai prediktorai; az internetaddikció és az egyéb viselkedési addikciók pszichológiai vonatkozásai.

Koronczai Beatrix

Klinikai szakpszichológus. Jelenleg az ELTE Pszichológiatudomány Doktori Iskola doktorjelöltje, doktori témája az internet-függőség. Munkatapasztalata van a gyermek- és serdülőterápiában, felnőtt pszichodrámacsoport vezetésében, iskolai drogprevencióban és drogprevenciók képzésében, valamint e-mailes és online tanácsadásban, állatasszisztált terápia vezetésében.

Rácz Bence

Nemzetközileg elismert információbiztonsági szakértő, főbb szakterületei az információbiztonsági auditok és etikus hackelési projektek vezetése, különös tekintettel az üzleti hírszerzésre és ennek elhárítására. A Magyar Detektív Szövetség tagja, a Nemzetközi Rendőrszövetség (IPA) pártoló tagja. A magánszektorban 1997 óta tevékenykedik, referenciái közt több külföldi vállalkozás mellett megtalálható a Magyar Informatikai Minisztérium is. 2007 óta a Fusiongate Kft. információbiztonsági vállalkozás ügyvezetőjeként és vezető tanácsadójaként dolgozik, ahol főként biztonsági auditokat, tanácsadást és etikus hackelési projekteket vezet.

Szabó Endre Győző

Jogász, környezetvédelmi szakjogász, adatvédelmi szakértő, a Közigazgatási és Igazságügyi Minisztérium (KIM) főosztályvezető-helyettese az Igazságügyi Együttműködési és Nemzetközi Magánjogi Főosztályon. Több mint hét éve foglalkozik adatvédelemmel, először a magyar adatvédelmi biztos munkatársa, majd az európai adatvédelmi biztos stábjának tagja nemzeti szakértőként Brüsszelben. 2007 óta ismét az Adatvédelmi Biztos Irodájában tevékenykedik főosztályvezető-helyettesként. Az adatvédelmi hatóságok közötti európai együttműködés keretében több nemzetközi munkacsoportban képviseli az adatvédelmi biztost.

Szabó György

Mérnök, térinformatikus, a Budapest Műszaki és Gazdaságtudományi Egyetem docense. Kutatási területe lefedi a tér regisztrálásával, modellezésével kapcsolatos tradicionális mérnöki és földtudományi területeket (mérnöki modellezés, geodézia, kartográfia, fotogrammetria, távérzékelés), valamint a földtudományok, térképészet, informatika integrációjával létrejött térinformatika műszaki, környezeti, társadalmi alkalmazásait. Számos térinformatikai témájú szakkönyv, tanulmány szerzője. A BME Építőmérnöki Karának 1983 óta oktatója. Ezenkívül szakirányú térinformatikai tárgyakat tanít a BME Gazdaságtudományi Karán és a Corvinus Egyetem Gazdaságinformatikus képzésében. Akadémiai tevékenysége mellett az utóbbi két évtizedben a Geomatik Kft. ügyvezetőjeként a térinformatika stratégiai, ipari feladatainak megoldásában is aktív szerepet vállalt.

Székely Iván

Társadalmi informatikus, az adatvédelem és az információs szabadság multidiszciplináris területeinek nemzetközileg ismert szakértője és kutatója, az OSA Archivum főtanácsadója, a BME docense. Kandidátus (szociológia). 1995 és 1998 között az új adatvédelmi biztos hivatal egyik alapítója és főmunkatársa. A BME mellett az ELTE Szociológiai Intézetében, a Közép-európai Egyetemen és a Budapesti Kommunikációs Főiskolán indított új, interdiszciplináris jellegű kurzusokat. Számos tanulmány és szakkönyv szerzője, szerkesztője; az IKT vonatkozású törvényhozás nemzetközi szakértője, kormányzati információs stratégiai dokumentumok társszerzője, a nyilvánosság és titkosság témakörével foglalkozó nemzetközi kutatócsoportok aktív résztvevője.

Talyigás Anikó

Matematika–informatika szakos tanár. Az újpesti Megyeri úti számítástechnika-tagozatos általános iskola, 2002 szeptembere óta a budapesti Madách Imre Gimnázium matematika–informatika szakos tanára. Az egyetem mellett végzett vezetőoktatói képzést az ISZE (Informatika-Számítástechnika Tanárok Egyesülete) keretein belül. 2005-ben kilenc kolléga számára akkreditált felnőttképzést tartott Számítógép- és internet-alapismeretek címmel.

Talyigás Judit

Villamosmérnök, politológus, az MTI Zrt. Adatbázisok és Archivumok igazgatója. A Budapesti Műszaki és Gazdaságtudományi Egyetemen elektronikus kereskedelmet tanít. Kiemelten fontosnak tartja a korszerű technikai, ezen belül informatikai rendszerek magas szintű tudományos ismeretterjesztését. Több fórumot, beszélgetést szervezett ennek érdekében. Számos, az információs társadalomról és az elektronikus kereskedelemről szóló könyv szerzője, szerkesztője. Legfontosabbak: *Tézisek az információs társadalomról* (2000), *E-világi beszélgetések.hu* (szerk.) (2004), *Az elektronikus kereskedelem* (2005), *Arcok a háló mögül* (szerk.) (2009). Elsősorban az informatika és az alkalmazáskutatás fejlesztési területeken dolgozott.

Turchányi Géza

Az 1970-es évek végén a KFKI-ban kezdett megismerkedni a számítógép-hálózatokkal, az 1980-as évek végén pedig a genfi CERN-ben az internettel. A magyar internet hőskorának 1991 óta szereplője, a WWW első magyar ismertetője, a KFKI Internet Klubjának társelnöke, az amszterdami RIPE NCC munkatársa, majd a Matáv Internet gerinchálózatának tervezője volt. Az *Arcok a háló mögül* (2009) című könyv szerzője.

Vajda Zsuzsanna

Pszichológus, egyetemi tanár, a Magyar Pszichológusok Egyesülete alapító elnöke. Főbb kutatási területe a gyermekek fejlődése és nevelése, a kultúra szülői szerepre, nevelésre gyakorolt hatása. Könyvei és tanulmányai jelentek meg a gyermekfelfogás alakulásáról, a változó szocializációs körülményekről, a szocializáció folyamatáról és intézményrendszeréről, ezen belül a digitális média szocializációra gyakorolt hatásáról. Több, a nevelés kérdéseit és gyakorlatát népszerű formában leíró könyve is megjelent. Korábban a Miskolci Egyetem pszichológia tanszékének vezetője, 2010 szeptemberétől a budapesti Corvinus Egyetem oktatója.

Z. Karvalics László

Történész, az információs társadalom kutatója, a Szegedi Tudományegyetem Könyvtár- és HumánInformáció-tudományi Tanszékének tanszékvezető egyetemi docense, az ITTK (Információs Társadalom- és Trendkutató Központ) volt igazgatója, örökös tiszteletbeli elnöke (2006-tól). Számos, az információs társadalommal és információtudománnyal foglalkozó kurzus kidolgozója, szakkönyv és tanulmány szerzője. Kar Kiváló Oktatója (1999), Széchenyi-ösztöndíjas (2000-től). Fontosabb könyvei: az internettel foglalkozó *Fogpiszkáló a hálózaton* (2000), *Az információs társadalom keresése* (2002), *Információ, társadalom, történelem* (2003), *Bevezetés az információtörténelembe* (2004). A könyvek és régi folyóiratok mellett szenvedélyesen gyűjt fadobozokat, fogpiszkálócsomagokat és -tartókat.

IRODALOM

Talyigás Judit: Bevezető

Barabási Albert-László, *Villanások – a jövő kiszámítható*, Budapest, Nyitott Könyvműhely, 2010.

Menzies, Gavin, *1421, amikor Kína felfedezte a világot*, Budapest, Alexandra, 2004.

MTI-hír, 2008. október 27.

Talyigás Judit (szerk.), *E-világi beszélgetések*, Budapest, Pesto, 2004.

Varga Csaba, *Jel jel jel avagy az abc 30000 éves története*, Budapest, Frig, 2001.

<http://einclusion.hu/2010-04-16/internet-penetracio-es-internet-hasznalat-2009-vegen/>

<http://olajkk.szoljon.hu/orszag-vilag/gazdasag/internethasznalat-a-vilagban-minden-amit-tudni-erdemes-285220>

Csepeli György: Veszélyesen élni? Avagy az internethasználat kockázatai

Bard, Alexander-Söderquist, Jan, *Netocracy*, London, Pearson Education, 2002.

Beck, U., *Világkockázat-társadalom. Az elveszett biztonság nyomában*, Szeged, Belvedere, 2008.

- Castells, M., *A hálózati társadalom kialakulása*, Budapest, Gondolat, 2005.
- Castells, M., *Az identitás hatalma. Az információs korszak*, II, Budapest, Gondolat, 2006.
- Castells, M., *Az évezred vége*, Budapest, Gondolat, 2007.
- Csepeli György, *Az információ a modern társadalomban*, *Jel-Kép*, 1985, 2.
- Csepeli György, *Álarcosbál a blogteremben*, *Kritika*, 2009/6, 3–5.
- Csepeli György–Prazsák Gergő, *Örök visszatérés. Társadalom az információs korban*, Budapest, Józsefvég, 2010.
- Ferguson, Niall, *A világ háborúja – A gyűlölet évszázadának története*, Budapest, Scolar, 2008.
- Hankiss Elemér, *Társadalmi csapdák. Diagnózisok*, Budapest, Magvető, 1983.
- Hankiss Elemér, *Csapdák és egerek. Magyarország 2009-ben és tovább*, Budapest, Manager-Médiavilág, 2009.
- Prensky, Marc, *Digital Natives, Digital Immigrants*, Part 1: *On the Horizon*, 2001, 9(5), 1–6; Part 2: *Do they really think differently?*, *On the Horizon*, 2001, 9(6), 1–6.
- Rogers, E. M., *Diffusion of Innovation*, Glencoe, Free Press, 1962.
- Simon H., *Korlátozott racionalitás. Válogatott tanulmányok*, Budapest, Közgazdasági és Jogi, 1982.
- Surowiecki, J., *A tömegek bölcsessége*, Budapest, Demos, 2007.
- Turing, Alan, *Computing machinery and intelligence*, *Mind*, 59(236), 1950, 433–460.
- Z. Karvalics László, *Információ, társadalom, történelem*, Budapest, Typo-text, 2003.

Rácz Bencze: We watch you watch

Gödel, Kurt, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme*, 1931.

**Székely Iván: Kukkoló társadalom
– avagy van-e még függöny virtuális ablakunkon?**

Bentham, Jeremy, *Panopticon, or the Inspection-House* (1787). Modern kiadása: Bozovic, Miran (szerk.), *The Panopticon Writings*, London, Verso, 1995, 29–95.

Feeley, Malcolm M.–Simon, Jonathan, The New Penology: Notes on the Emerging Strategy of Corrections and its Implications, *Criminology*, 30(1992), 449–474.

Flash Eurobarometer 225: The Gallup Organization: *Data Protection in the European Union. Citizens' perceptions. Analytical Report*. European Commission, 2008.

Goold, Benjamin J., Privacy, Identity and Security, in Uő–Lazarus, Liora (szerk.), *Security and Human Rights*, Oxford–Portland, Hart Publishing, 2007.

Lessig, Lawrence, *Code and Other Laws of Cyberspace*, New York, Basic Books, 2000.

Lyon, David (szerk.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London–New York, Routledge, 2003.

Manifesto for CCTV filmmakers (2007). http://www.ambienttv.net/2007/manifestoforCCTVfilmmakers_screen.pdf

Mann, Steve–Nolan, Jason–Wellman, Barry, Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments, *Surveillance and Society*, 1(3), 2003, 331–355.

McCahill, Michael–Norris, Clive, *CCTV in Britain*. Berlin, 2003, Urban Eye. http://www.urbaneye.net/results/ue_wp3.pdf

Rotenberg, Marc–Knight, Allison–Pereda, Katitza Rodriguez (szerk.), *Privacy and Human Rights. An International Survey of Privacy Laws and Developments*, Washington–London, EPIC, Privacy International, 2006.

Székely Iván, *Az adatvédelem és az információs szabadság filozófiai, jogi, szociológiai és informatikai aspektusai*, kandidátusi értekezés, Budapest, 1994.
Székely Iván, Az adatvédelmi biztos első féléve, *Magyar Távközlés*, VII(1996)/4, 3–6.

Vincze Beatrix, A magánszféra védelme a modern japán információs technológiában, in Székely Iván–Szabó Máté Dániel (szerk.), *Szabad adatok*,

védett adatok, 2, Budapest, Információs Társadalomért Alapítvány, 2008, 215–230.

Warren, Samuel D.–Brandeis, Louis D., The Right to Privacy, *Harvard Law Review*, 4(1890); magyarul Uők, A magánszférához való jog, *Információs Társadalom*, V(2005)/2, 7–31.

Demetrovics Zsolt–Koronczai Beatrix:

Az internetfüggőség néhány pszichológiai vonatkozása

Aboujaoude, E.–Koran, L. M.–Gamel, N.–Large, M. D.–Serpe, R. T., Potential Markers for Problematic Internet Use: A Telephone Survey of 2,513 Adults, *CNS Spectrums*, 11(10), 2006, 750–755.

Armstrong, L.–Phillips, J. G.–Saling, L. L., Potential determinants of heavier Internet usage, *International Journal of Human Computer Studies*, 2000, 53, 537–550.

Bayraktar, F.–Gün, Z., Incidence and correlates of Internet usage among adolescents in North Cyprus, *Cyberpsychology and Behavior*, 2005, 10(2), 191–197.

Bessiere, K.–Kiesler, S.–Kraut, R.–Boneva, B. S., Effects of internet use and social resources on changes in depression, *Information, Communication & Society*, 2008, 11(1), 47–70.

Bostwick, J. M.–Bucci, J. A., Internet sex addiction treated with naltrexone, *Mayo Clinic Proceedings*, 2008, 83(2), 226–230.

Caplan, S. E., Problematic Internet use and psychosocial well-being: Development of a theory-based cognitive-behavioral measurement instrument, *Computers in Human Behavior*, 2002, 18, 553–575.

Caplan, S. E., A Social Skill Account of Problematic Internet Use, *Journal of Communication*, 2005, 55(4), 721–736.

Chou, C.–Condrón, L.–Belland, J. C., A Review of the Research on Internet Addiction, *Educational Psychology Review*, 2005, 17(4), 363–388.

Csepeli György, *Szociálpszichológia*, Budapest, Osiris, 1997.

- Davis, R. A., A cognitive-behavioral model of pathological Internet use, *Computers in Human Behavior*, 2001, 17, 187–195.
- Dell'Osso, B.–Hadley, S.–Allen, A.–Baker, B.–Chaplin, W. F.–Hollander, E., Escitalopram in the treatment of impulsive-compulsive internet usage disorder: an open-label trial followed by a double-blind discontinuation phase. *J Clin Psychiatry*, 69(3), 452–456.
- Demetrovics Zsolt–Koronczai Beatrix–Kun B., Internetfüggőség és problémás internethasználat, in Demetrovics Zsolt–Kun B. (szerk.), *Az addiktológia alapjai*, IV, Budapest, Eötvös, 2010, 253–269.
- Demetrovics Zsolt–Kun B., Viselkedési addikciók, in Demetrovics Zsolt (szerk.), *Az addiktológia alapjai*, I, Budapest, Eötvös, 2007, 133–225.
- Demetrovics Zsolt–Kun B., A viselkedési függőségek és az impulzuskontroll egyéb zavarainak helye az addikciók spektrumán, in Uők (szerk.), *Az addiktológia alapjai*, IV, Budapest, Eötvös, 2010, 29–40.
- Demetrovics Zsolt–Nyikos E.–Szeredi B., A Problémás Internethasználat Kérdőív bemutatása, *Psychiatria Hungarica*, 2004, 19(2), 141–160.
- Demetrovics Zsolt–Rózsa S.–Szeredi B., The three-factor model of Internet addiction: The development of the Problematic Internet Use Questionnaire, *Behavior Research Methods*, 2008, 40(2), 563–574.
- Douglas, A. C.–Mills, J. E.–Niang, M.–Stepchenkova, S.–Byun, S.–Ruffini, C.–Lee, S. K.–Loutfi, J.–Lee, J. K.–Atallah, M.–Blanton, M., Internet addiction: Meta-synthesis of qualitative research for the decade 1996–2006, *Computers in Human Behavior*, 2008, 24, 3027–3044.
- Griffiths, M. D., Internet addiction: Does it really exist?, in Gackenbach, J. (szerk.), *Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implications*, New York, Academic Press, 1998.
- Holden, C., Psychiatry. Behavioral addictions debut in proposed DSM-V, *Science*, 327(5968), 935.
- Johansson, A.–Götestam, K. G., Internet addiction: characteristics of a questionnaire and prevalence in Norwegian youth (12–28 years), *Scandinavian Journal of Psychology*, 2004, 45(3), 223–9.
- Kim, H.-K.–Davis, K. E., Toward a comprehensive theory of problematic Internet use: Evaluating the role of self-esteem, anxiety, flow, and the self-rated importance of Internet activities, *Computers in Human Behavior*, 2009, 25, 490–500.

- Kim, K.-Ryu, E.-Chon, M.-Y.-Yeun, E.-J.-Choi, S.-Y.-Seo, J.-S.-Nam, B.-W., Internet addiction in Korean adolescents and suicidal ideation: A questionnaire survey, *International Journal of Nursing Studies*, 2006, 43(2), 185–192.
- Kraut, R.-Kiesler, S.-Boneva, B.-Cummings, J. N.-Helgeson, V.-Crawford, A. M., Internet paradox revisited, *Journal of Social Issues*, 2002, 58(1), 49–74.
- Kraut, R.-Lundmark, V.-Patterson, M.-Kiesler, S.-Mukopadhyay, T.-Scherlis, W., Internet Paradox: a social technology that reduces social involvement and psychological well-being?, *American Psychologist*, 1998, 55, 1017–1031.
- LaRose, R.-Eastin, M. S.-Gregg, J., Reformulating the Internet paradox: Social cognitive explanations of Internet use and depression, *Journal of Online Behavior*, 2001, 1(2).
- Li, S.-M.-Chung, T.-M., Internet function and Internet addictive behavior. *Computers in Human Behavior*, 2006, 22, 1067–1071.
- Mitchell, P., Internet addiction: Genuine diagnosis or not?, *Lancet*, 2000, 355, 632.
- Morahan-Martin, J.-Schumacher, P., Incidence and correlates of pathological Internet use among college students, *Computers in Human Behavior*, 2000, 16, 13–29.
- Murali, V.-George, S., Lost online: an overview of internet addiction, *Advances in Psychiatric Treatment*, 2007, 13, 24–30.
- Nalwa, K.-Anand, A. P., Internet addiction in students: A cause of concern, *Cyberpsychology and Behavior*, 2003, 6(6), 653–656.
- Niemz, K.-Griffiths, M.-Banyard, P., Prevalence of pathological Internet use among university students and correlations with self-esteem, the General Health Questionnaire (GHQ), and disinhibition, *Cyberpsychology and Behavior*, 2005, 8(6), 562–570.
- Nyikos E.-Szeredi B.-Detrovics Zsolt, Egy új viselkedéses addikció: Az internethasználat személyiségpszichológiai korrelátumai, *Pszichoterápia*, 2001, 10, 168–182.
- Orzack, M. H.-Orzack, D. S., Treatment of computer addicts with complex co-morbid psychiatric disorders, *Cyberpsychology and Behavior*, 1999, 2(5), 465–473.

- Rice, L.-Markey, P. M., The role of extraversion and neuroticism in influencing anxiety following computer-mediated interactions, *Personality and Individual Differences*, 2009, 46, 35-39.
- Shapira, N. A.-Goldsmith, T. D.-Keck, P. E.-Khosla, U. M.-McElroy, S. L., Psychiatric features of individuals with problematic internet use, *Journal of Affective Disorders*, 2000, 57, 267-272.
- Treuer, T.-Fabian, Z.-Furedi, J., Internet addiction associated with features of impulse control disorder: Is it a real psychiatric disorder?, *Journal of Affective Disorders*, 2001, 66, 283-239.
- Van den Eijnden, R. J.-Meerkerk, G. J.-Vermulst, A. A.-Spijkerman, R.-Engels, R. C., Online communication, compulsive Internet use, and psychosocial well-being among adolescents: a longitudinal study, *Developmental Psychology*, 2008, 44 (3), 655-665.
- Whang, L. S.-M.-Lee, S.-Chang, G., Internet Over-Users' Psychological Profiles: A Behavior Sampling Analysis on Internet Addiction, *Cyberpsychology and Behavior*, 2003, 6(2), 143-149.
- Young, Kimberley S., *Caught in the Net: How to recognize the signs of Internet addiction - and a winning strategy for recovery*, New York, Wiley, 1998.
- Young, Kimberley S., Internet addiction: The emergence of a new clinical disorder, *Cyberpsychology and Behavior*, 1998, 1(3), 237-244.
- Young, Kimberley S., Internet Addiction: Symptoms, Evaluation, and Treatment, in VandeCreek, L.-Jackson, T. (szerk.), *Innovations in Clinical Practice: A Source Book*, 17, 19-31, Sarasota, FL, Professional Resource Press, 1999.
- Young, Kimberley S.-Pistner, M.-O'Mara, J.-Buchanan, J., Cyber disorders: The mental health concern for the new millennium, *Cyberpsychology and Behavior*, 1999, 2(5), 475-479.

**Z. Karvalics László: Az univerzális kvantor rémuralma
– avagy a veszélydiskurzusok logikai szerkezetéről**

Morozov, Evgeny, *Think Again: The Internet*, lásd http://www.foreignpolicy.com/articles/2010/04/26/think_again_the_internet – letöltve: 2010. június 9.

The Death of Human Understanding Computer, 2008. október, 41. évf. 108, 106–107.

<http://axel.hu/cikk/axel.hu/19188>

http://index.hu/kultur/klassz/2010/04/25/a_google_konyvzabalo_kis-gomboc/

<http://portal.ujember.hu/hetilap/100117/10/internet>

Talyigás Anikó: Az informatikaoktatás dinamikája

<http://www.nefmi.gov.hu/kozoktatas/2010-evi-majus-juniusi>

<http://www.oh.gov.hu/kozoktatas/kapcsolodo-jogszabaly/2010-januar-1-tol> – informatika vizsgakövetelmény

<http://www.microsoft.com/hun/protect/default.msp>

<http://www.doza-kkmsa.sulinet.hu/rgazda/index.html#link1>

http://ec.europa.eu/education/languages/eu-programmes/doc201_hu.htm

<http://www.snopes.com/inboxer/hoaxes/hoaxes.asp#computer>

http://ec.europa.eu/education/languages/eu-programmes/doc201_hu.htm

Vajda Zsuzsanna: A gyerekek és a számítógép

Attevel, P.–Suazo-Garcia, B.–Battle, J., Computers and Young Children: Social Benefit or Social Problem?, *The Future of Children*, 2008(18), tavasz.
Bayer Judit, Az internetkorlátozás a kereskedelmi szféra eszközeivel: szűrők és felbukkanó ablakok. A gyermekekre káros internettartalom egyes kérdései, *Médiakutató*, 2005. nyár, 32–41.

Bors Réka, Pro anorexia fórumok. Az evészavarok kommunikációs aspektusai, *Médiakutató*, 2009. ősz, 23–35.

Forgács Attila, Médiaüzenetek és évezavarok, lásd http://www.elitmed.hu/upload/pdf/mediauzenetek_evezavarok-1725.pdf – letöltve: 2010. május 25.
Greenfield, P., *School children's chat rooms*, az UCLA honlapján – letöltve: 2009. december 21.

Hammer F., A veszély archeológiája. A számítógép és a gyerekek esete, *Médiakutató*, 2006. ősz, 20–50.

Jordan, A. B., Children's Media Policy, *The Future of Children*, 2008(18)/1, tavasz.

Kirkorian, H.–Wartella, E.–Anderson, D., Media and Young Children's Learning, *The Future of Children*, 2008(18)1, tavasz.

Levesque, R. J. R., *Adolescents, Media and the Law. What Developmental Science Reveals and Free Speech Requires*, Oxford University Press, 2004.

McNeal, J.–Yeh, C., Born to Shop, *American Demographics*, 1993, 34–39.

Roberts, D.–Foehr, U. G., Trends in Media Use, *The Future of Children*, 2008(18)/1, tavasz.

Schmidt, M. E.–Vandewater, E., Media and Attention, Cognition and School Achievement, *The Future of Children*, 2008(18)/2, nyár.

Strasburger, V. C.–Wilson, B.–Jordan, A. B., *Children, adolescents and media*, Los Angeles–London, Sage, 2009.

Török B., *Számítógéphasználat óvodáskorban. Egy országos szülővizsgálat tapasztalatai*, Budapest, 2002, lásd www.oki.hu

Valentine, G.–Holloway, S.-L., Cyberkids? Exploring Children's Identities and Social Networks in Online and Off-line Worlds, *Annals of the Association of American Geographers*, 2002/2.

Wartella, E. A.–Jennings, N., Children and Computers: New Technology. Old Concerns. The Future of Children, *Children and Computer Technology*, 2000(10)/2, ősz–tél.

www.standard-team.hu/internet-penetracio-2008-1.html.

Szabó György: Virtuális világ és valós tér. Utópiák, realitás, veszélyek

Baker, S., *Numerátorok*, Budapest, Geopen, 2009.

Brimicombe, A., Location-Based Services and Geo-Information Engineering, London, Wiley-Blackwell, 2009.

Czinkóczy A.–Szabó György, *Mobile Technologies for Modeling Urban Space Allocation in Real Time*, ISPRS Archive Vol. XXXVIII, Part 4-8-2-W9, Core Spatial Databases – Updating, Maintenance and Services – from Theory to Practice, Haifa.

Czinkóczy A.–Szabó György, *Bicycle Road Optimization Using RFID Tags, Street Computing*, in *OZCHI: Human-Computer Interaction Conference*, Melbourne.

Detrekői Á.–Szabó György, *Térinformatika*, Budapest, Nemzeti Tankönyvkiadó Rt., 2002.

Dodge, M.–Smith, A.–Doyle, S., *Urban Science, GIS Europe*, 1997(6)/10. Dömölki Bálint (szerk.), *Égen-Földön Informatika*, Budapest, Typotex, 2008.

Erdős G., *Akcióelmélet*, Budapest, Magvető, 1986.

Frank, A. U., *Ontology. A consumer's point of view*, 2008, lásd http://www.dpi.inpe.br/geopro/referencias/ontology_af.pdf

Imrédi-Molnár László, *Térképalkotás*, Budapest, Tankönyvkiadó, 1970.

Kállai J., *A téri tájékozódás és a szorongás*, Budapest, Janus–Gondolat, 2004.

Kállai J.–Karádi K.–Tényi T., *A térelmény kultúrtörténete és pszichológiája*, Budapest, Tertia, 1988.

Krugman P., *Földrajz és kereskedelem*, Budapest, Nemzeti Tankönyvkiadó, 2003.

Langran, K., *Time in Geographic Information Systems*, London, Taylor and Francis, 1993.

Láng J., *A mitológia kezdetei. Az ősi népek elbeszélései*, Budapest, Gondolat, 1979.

Madden, M., *Manual of Geographic Information Systems*, Bethesda, ASPRS, 2009.

Mészáros, R., *A kibertér és ami körülötte van*, Szeged, JATEpress, 2008.

Neutens, T.–Witlox, F.–Demaeyer, P., Individual accessibility of travel possibilities, *EJTIR*, 2007(7)/4.

Peuquet, D. J., *Making Space for Time: Issues in Space-Time Data Representation*, *Geoinformatica*, 2001, 5, 11.

Raisz, E., *General Cartography*, New York, McGraw–Hill Book Co. 1948.

Rozsak, T., *Az információ kultusza*, Budapest, Európa, 1990.

Szabó György, Tér, Idő, Hely – Globális, regionális, és lokális terek modellezése, *Geomatikai Közlemények*, XIII, MTA GGKI, Sopron, 2010.

Weaver, W., Újabb adalékok a hírközlés matematikai elméletéhez, in Shannon, C. E.–Weaver, W., *A kommunikáció matematikai elmélete*, Budapest, OMIK, 1986.

Shapiro C.–Varian, H. R., *Az információ uralma*, Budapest, Geomédia, 2000.

Tószegi Zsolt, *A képi információ*, Budapest, 1994 (Az Országos Széchényi Könyvtár Füzetek, 6).

<http://plato.stanford.edu/entries/mereology/> (First published Tue May 13, 2003; substantive revision Thu May 14, 2009)

<http://thenextweb.com/2008/08/07/google-plants-forests-in-holland-amateurish-censorship-in-maps/>

www.kisalfold.hu, 2010.07.01.

TÁRGYMUTATÓ

A

absztinencia 119, 125, 132
 adatalany 43, 48, 50, 57, 62, 64, 115
 adatbányászat 61, 62, 95, 224
 adatbázis 16, 18, 31, 32, 33, 63, 69,
 81, 83, 89, 92, 153, 200, 204, 230
 adatbázis-kezelés 150
 adatbiztonság 46, 116
 adatgyűjtés 13, 17, 61, 105, 196, 199, 202
 adathalászat 136
 adathordozó 22, 31, 32, 91
 adatigény 45, 63
 adatkezelő 46, 48, 57, 59, 61, 114, 116
 adatmanipuláció 20
 adatmegőrzés 62, 63
 adatminimum elve 46, 47
 adatmódosulás 32
 adatok alanya 48, 227
 adatromlás 32
 adattárház 95
 adatvédelem 93, 110, 226, 228
 adatvédelmi törvény 46, 47, 57,
 58, 111, 112, 114, 116
 adatvédő 22
 adatvesztés 32
 aktuárius társadalom 107
 anonim közösség 40
 anonimitás 97, 129, 169, 228
 arctalanság 50, 51, 55, 56, 57, 134

auditor 77, 225
 automatikus szűrőrendszer 13
 azonosítás 46, 51, 57, 68, 69, 72, 73, 74,
 75, 81, 224, 228

B

behatolásteszt 77
 banki rendszer 34
 bírósági ítélet 18, 223
 bizalmas adat 91, 182
 bizalom 14, 15, 23, 63, 65
 biztonságérzet 195
 biztonsági incidens 67, 68, 70
 biztonságtechnika 76, 91
 blackhat 76, 79, 80, 83
 blog 12, 20, 22, 92, 140, 219, 228
 blogger 140
 botnet 31, 86, 220
 brute force 72, 73, 74

C, CS

célhoz kötöttség 46, 47, 49, 62, 63, 223
 chat 22, 81, 82, 126, 127, 128, 135, 151,
 155, 156, 159, 161, 162, 163, 164, 176
 cookie-irtó 118, 228
 cracker 76, 77, 79, 80, 145
 cyber-bullying 136, 230
 családi fotó 18, 32

D

Ddos 84, 85, 86, 87, 225
 Deep Web 135, 230
 dekódoló algoritmus 82
 digitális bennszülött 38, 148, 221, 232
 digitális bevándorló 38, 148, 221
 digitális egyenlőtlenség 35
 digitális gyűjtemény 18
 digitális kamera 38, 199
 digitális szakadék 35, 180, 181
 digitális város 201
 downtime 84
 döntéstámogató szoftver 39

E

ECDL-modul 150
 egyedüllet 17, 19, 96, 129
 e-kereskedelem 105
 elektronikus aláírás 74, 224
 etika 20, 41, 109, 115, 116, 153,
 160, 227

F

Facebook 19, 82, 92, 102, 182
 felekezeti hovatarozas 49, 223
 fórum 17, 20, 50, 86, 151, 155, 156,
 158, 184, 185, 190, 227
 fuzzy 41

G, GY

Google 39, 92, 101, 134, 203,
 204, 230
 GPS 39, 195, 199, 201, 202, 233, 234
 greyhat 76, 79, 80
 gtalk 81, 82, 92
 Gutenberg-galaxis 12, 38
 gyereknevelés 14

H

hacker 11, 67, 68, 69, 70, 75–91,
 145, 225
 hackertámadás 84
 helymeghatározás 193, 195, 198, 199,
 201, 202, 234
 híresztelés 51, 55
 hoax 136, 159, 230

I

identitáslopás 32, 103, 136
 információbiztonság 70, 77, 91, 225
 információlopás 34, 76
 információs önbíráskodás 55
 információs önrendelkezés 195, 204
 információs önrendelkezési jog 43, 44,
 48, 50, 52, 53, 54, 64
 információs társadalom 9, 35, 38, 41,
 42, 94, 108, 115, 153, 157,
 200, 201, 202, 222, 226
 információszerzés 99, 100, 126
 informatikaérettségi 152
 informatikai bűnözés 33
 informatikaoktatás 149, 164
 infrastruktúra 31, 32, 41, 73, 75, 84, 85,
 87, 90, 117, 197, 214, 220
 innovátor 35, 36
 interakció 127, 129, 182, 201
 internetpenetráció 85
 internetaddikció 121, 122, 236
 internetfüggőség 11, 121–132
 internethasználat 10, 11, 16, 24, 25, 35,
 38, 92, 97, 100, 103, 122–132, 155,
 168, 177, 178, 181, 210, 212, 219
 internetkutató 135, 136, 141
 internetszolgáltatás 208, 209, 212
 IPv4 207, 216
 IPv6 207, 216, 217

J

játékfüggőség 132, 136
 játékportál 17
 játékszenvedély 123
 jelszó 16, 22, 45, 67–75, 81, 91, 92,
 162, 220
 jogellenes adatkezelés 53

K

kapcsolati háló 16, 88
 kémprogram 31, 102, 220, 228
 képpalkotás 197
 képességfejlesztő 19
 képi információk 196, 197
 keylogger 31
 kiberháború 80

- kiberhadviselés 86–87
 kiberkriminológia 34
 killer application 35, 221
 kiszolgáltatottság 11, 12, 20, 26,
 59, 187, 194
 kockázatiipar 107
 kommunikációs háló 26, 30, 101, 202
 koncentrálokésztség 138, 139
 könyvtár 16, 17, 31, 96, 153, 157, 209
 közfeladat 40, 41
 közösségi hálózat 102, 229
 közösségi oldal 15, 16, 17, 19,
 20, 21, 22, 49–52, 56, 58,
 67, 68, 82, 161, 182
 közösségszervező 21
 közszereplő 20, 102
 kulcspár 74, 75
 kulturális gazdag 36, 37
 kulturális szegény 36, 37
 különleges adat 34, 49, 223
- L
 laptop 38, 81, 167, 211, 212, 214
 levéltár 17
 loginnév 70, 71, 73
- M
 magánkulcs 225
 magánélet 96, 97, 99, 114, 116, 119,
 120, 144, 169, 227, 228
 magánszféra 60, 61, 65, 96–97,
 98–100, 111, 118, 226
 magánterület 99
 magánügy 99
 magányos 130, 131
 média 21, 22, 34, 35, 38, 41, 42,
 75, 76, 77, 80, 114, 134, 145, 146,
 167, 169, 172, 173, 174, 175, 179–191
 médiatartalom 146
 megbízhatóság 12, 15
 megfigyelőautomata 100
 mobil navigáció 201
 mobilinternet 209, 212, 213, 215
 mobiltelefon 38, 71, 74, 75, 92, 101,
 168, 179, 190, 211, 230, 233
 MSN 81, 82, 92, 164
- munkáltató 56–60, 112, 114
 munkavállaló 56–60, 223
- N, NY
 netbankolás 44, 47, 73, 85
 netizen 35
 netproletár 35
 netokrata 35
 nicknév 155
 nym-generátor 118, 228
 nyilvános fórum 116, 151
 nyilvános kulcs 225
- O
 online casino 84
 online hír 12
 online játék 126, 127, 132
- Ö
 önbíráskodás 17, 55–56
 önkorlátozás 60
 önkormányzat 14, 46, 47
 önrendelkezés 43, 44, 48, 50, 52, 53, 54,
 64, 97, 98, 99, 120, 195, 204, 227, 228
 önszabályozás 12, 20, 41, 189
 örök nyilvánosság 48, 55
- P
 pánikdiskurzusz 147
 pánikjelenség 146
 pendrive 18, 22
 PET 116, 117, 118
 ping flood 86
 pornográf 34, 126, 136, 187–189, 233
 programféreg 31
 publikus script 86
- R
 RFID 118, 195, 198, 201, 202, 228, 233
- S
 script kid 76, 77, 79, 80
 shoulder surfing 71
 Skype 17, 81, 82
 spam 65, 86, 104, 105, 106, 115, 136,
 220, 228

statisztika 23–24, 61, 74, 108, 122,
208, 210, 213, 220
stratégiai játék 135, 156

SZ

számítástechnika 14, 90, 150, 168,
169, 172, 176, 177, 180, 181, 185, 230
számítógépes vizsgáztatás 13
szélessávú internet 30, 208, 209, 210,
211, 212, 214
személyes adat 13, 43–65, 71, 83,
99, 102, 117, 161, 194, 204, 220,
222, 223, 224, 226, 227
személyi adatok védelme 11, 43–65,
99, 222, 226
személyiség védelme 54, 97
személyiségprofil 68, 83, 89
szenvédélybetegség 136
szerzői jog 34, 65, 153, 188

T

társkereső/párkereső 15, 51, 155
távérzékelés 197, 199
távkorrepetálás 164
távoli eljáráshívás 31
térbeli adatkészlet 194, 202
térinformatika 11, 23, 194, 195,
198, 202
terrorfenyegetés 29
torrentoldal 134, 230

trójai program 31
tudást adó 19
tűzfal 16, 232
Twitter 22, 92

Ü

Ügyfélkapu 45, 51
üzleti hírszerzés 76, 82

V

vesélydiskurzus 105, 133–148
videodeficit 173
vírus 31, 92, 155, 161, 220
viselkedészavar 122

W

web 2.0 34, 38, 54, 58, 82, 219, 228
webpoloska 100, 102
webpoloskairtó 118
whitehat 76, 77, 79
WIFI 80–81, 92, 195, 198, 199, 201,
202, 213, 233

Y

YouTube 182

Z

zaklatás 51, 219, 230
zavarkeltés 33
zombihálózat 31

Tudás – elkötelezettség – felelősség



**Neumann János
Számítógép-tudományi Társaság**

Digitális Esélyegyenlőség

www.njszt.hu www.ecdl.hu

eVITA

njszt

DE!
Digitális
Esélyegyenlőség

Szüksége van rá!

10 millió vizsgázó a világ 148 országában már bizonyítja!

Jelentkezzen Ön is még ma az ország 400 vizsgaközpontjának egyikében!

segítség a
munkaerőpiacon

eredményesebb
munkavégzés

nemzetközi
versenyképesség

nem csak 20
éveseknek...

ECDL

Európai Számítógép-használói Jogosítvány

TM



ECDL
Magyarország



www.ecdl.hu

