Polgári Szemle, 13. évf., 4–6. szám, 2017, 173–183., DOI: 10.24307/psz.2017.1214

Kollár Csaba

Emlékeink lenyomatainak információbiztonsága

Hogyan őrizhetőek meg és írhatóak át emlékeink a digitális korban?

Information Security Regarding the Imprint of Our Memories

How Can They Be Preserved and Transcribed in Digital Age?

Összefoglalás

A digitális kort megelőző korokban emlékeink lenyomatai viszonylag biztonságban voltak. A tárgyakra vigyáztak, megvédték azokat a természeti károktól, mentették a háborúk és a vándorlások során, s így a képek, fényképek, írások, használati és egyéb tárgyak számos generáció számára jelentették a családi, a közösségi, de akár a nemzeti emlékezés biztos tárgyi bizonyítékait. A digitális korban ugyan a klasszikus emlékek megmaradtak, de arányait tekintve a digitális eszközökkel előállított és/vagy rögzített lenyomatok kerültek túlsúlyba. A lenyomatok egyfelől sokkal könnyebben készíthetőek el, másfelől sokkal nagyobb veszélynek vannak kitéve. Igaz, hogy ami egyszer a hálózatra felkerült, az gyakorlatilag örökre ott marad, mint egyfajta digitális lenyomat, de ezen dokumentumaink fölött elveszíthetjük a kontrollt, a tulajdont. A tanulmány – mely szekunder források elemzésén alapszik – bemutatja emlékeink lenyomatainak alapvető humán információbiztonsági lehetőségeit és módszereit, valamint a közeljövőben elterjedő technikákra épülő emlékbizonytalanság útjait is.

Dr. Kollár Csaba, PhD, oktató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola (kollar.csaba@uni-nke.hu).

Journal of Economic Literature (JEL) kódok: O15, Z1
Kulcsszavak: információbiztonság, emlékek, digitális kor

Summary
The imprints of memories in the era before digital age were relatively safe. The objects were guarded; protected from damages caused by nature; saved during wars and migration; thus the pictures, photos, papers, writings, utensils and other objects could be the sound material evidence of family, community or even national recollection for multiple generations. The classic memories still exist in the digital age, but in terms of proportion, the imprints produced and/or recorded with digital devices dominate. On the one hand, the imprints can be produced much more easily and, on the other hand, they are at much greater risk. It is true that if something is uploaded to the network, it will stay there forever, as some sort of digital imprint. People, however, lose control over and ownership of these documents. The study – based on the analysis of secondary sources – introduces the basic human information security opportunities and methods regarding the imprints of our memories as well as the ways of memory insecurities built on the techniques, which are going to expand in the near future.

Journal of Economic Literature (JEL) codes: O15, Z1
Keywords: information security, memories, digital age

Bevezetés – ingatag emlékeink

Tanulmányomat egy, a Facebookon terjedő mémmel szeretném indítani, mely azt hirdeti, hogy az emlék az egyetlen dolog, amit soha nem vehet el tőlünk senki. Az ismeretlen forrásból származó (bár a citatum.hu oldalon egy hasonló idézetet Jankó Olga írónőnek tulajdonítanak) – s így akár tudománytalannak is nevezhető – mondat megtalálása mögött is felfedezhetjük az internetnek és a Google-nak azt a tulajdonságát, hogy elfelejtett emlékeink visszahozásában vagy bizonytalan visszaemlékezéseink bizonyosabbá tételében a nevezett technikák milyen hasznosak lehetnek a számunkra. Elég csupán a keresőben megadni néhány kulcsszót, s máris érkezik a releváns és valid válasz. Kérdés persze, hogy a válaszok mennyire relevánsak és validak…

Lukacs (2012) könyvének ismertetőjében olvasható: „Kultúránk válsága közepette, amikor egy egész korszak ér véget, a történetírásban is bizarr jelenségeket látunk: kérészéletű divatirányzatokat, »hóbortokat«, hamisításokat". Ha a tömegmédia elterjedésétől vizsgáljuk az *átírások* és *újraírások* kérdését, akkor megállapíthatjuk, hogy a politikai marketingben (Newman, 2000), a gerillamarketingben (Levinson–McLaughlin, 2005), illetve az újabb irányzatok közül többek között a személyes márkaépítésben (Schawbel, 2012; Purkins–Royston-Lee, 2010) egyaránt találkozhatunk azzal a jelenséggel, hogy az objektívnek tekinthető tények egy része vagy nem jelenik meg az egyén önéletrajzában, vagy kreált tények alapján egy hamis, ámde a közvélemény számára

szimpatikus és vonzó életutat építenek fel. Rendszeresen lehet találkozni olyan véleményekkel, hogy a Wikipédia – amit gyakran még az oktatásban is felhasználnak mint elektronikus enciklopédia – szócikkeinek szerkesztői nem az objektív tények, hanem a gazdasági, társadalmi, politikai, jogi érdekek mentén szerkesztik a címszavakat. Ezeket a címszavakat aztán átveszik más adatbázisok (lásd Index, 2013), s így a hazugság megosztva és sokszorozva már az igazság látszatát képes kelteni. A megbízó elvárásai szerint dolgozó krónikások révén a történelmi emlékezetben gyakran már csak a „kozmetikázott", meghamisított tényekre fogunk emlékezni, s magától értetődőnek vesszük, hogy ez az emlékezet egyben az igazság is.

Az előzmények között található a *törlés* és a *megsemmisítés,* amikor végérvényesen semmisítenek meg valamilyen adatot, információt vagy magát az emlékhordozót. Ez a tömegmédia előtti korokban lehetett pl. a könyvek, a krónikák, a levelek, az iratok, az okmányok vagy az őrzésükre kijelölt épületek felgyújtása, a digitális korban pedig lehet egy egyszerű Del parancs is. Természetesen az az axióma, miszerint ami egyszer felkerült a hálózatba, az örökre ott marad, a törlés ellenére is igaz, hiszen a fájlok előzményei a szervereken tárolódnak, s kicsi az esélye annak, hogy a mentett és tükrözött tartalmak adathordozói végérvényesen tönkremennek. A digitális korban a törlést és a megsemmisítést – ez utóbbinál az összehangolt terrorcselekményeket vagy a tudatosan előírt selejtezést/megsemmisítést leszámítva, amikor közel egy időben valamennyi adathordozó megsemmisül, s így nincs lehetőség másolat készítésére – inkább úgy lehet értelmezni, hogy az internetet böngésző közönség számára válik elérhetetlenné az adott adat, információ. Megjegyzem, hogy a weblapokra feltett s onnan törölt információk egy része több-kevesebb sikerrel fellelhető a https://archive.org/web/ oldalon.

Az álló- és mozgóképek manipulálása, a rajta levő *információk retusálása* (vagy még korábban az eladósorba került hercegkisasszonyok festett portréjának a realitáson messze túlmutató szépsége) gyakorlatilag már az első felvételek elkészítése során felmerült igényként. Szinte valamennyi filmes megtanulja, hogy mit jelentenek a kameraállások, a felvételi szögek, a térbeliség, milyen kifejező ereje van a képkivágásoknak, illetve milyen trükköket lehet/kell alkalmazni akár a helyszínen, akár az utómunka során (Féjja, 1982). A digitális korban viszonylag egyszerű feladatnak számít a képről bizonyos tartalmak eltüntetése, vagy éppen az eredetileg rajta nem lévő információk rászerkesztése, s az igazán ügyes szoftveres grafikusok munkáján nem vagy csak hosszas elemzés során lehet észrevenni ezeket a manipulációkat.

Nem értjük (pontosan), hogy hogyan működik az elme (Pinker, 2002), de feltételezhetjük, hogy nagy valószínűség szerint az *álmok,* különösen a regressziós, tehát életünk korábbi szakaszában játszódó álmok is képesek gazdagítani hamis emlékképeinket. Az álmokhoz hasonló, de tudatosabb hatás érhető el *hipnózis*ban, azon belül is regressziós hipnózisban (Hewitt, 2008). Ilyenkor az alanyt visszaviszik életének egy korábbi részébe, ahol nemcsak újból átélheti és így feldolgozhatja a traumát (ha ez a terápia célja), de elhelyezhetőek olyan emlékek is, amelyekről az alany éber állapotában meggyőződéssel fogja állítani, hogy igazak. Az álmok és a hipnózis mellett a *média* és a *propaganda* is képes hamis emlékeket előállítani. Göbbels úgy vélekedett, hogy ha egy

hazugságot folyamatosan ismétlünk, akkor az emberek előbb-utóbb elhiszik. Ha pedig elég hangosan és sokan mondják, akkor (szinte) mindenki elhiszi, hogy úgy van. Mivel nincs lehetőségünk minden egyes – akár a számunkra, fejlődésünk szempontjából is fontos – eseményen és történésnél jelen lenni, ezért gyakran hagyatkozunk a média által közvetített beszámolókra, hírekre, rendszerint nem vizsgálva a hírek valódiságát. Ezek a hírek pedig később, ha felidézzük őket, már valós(nak hitt) emlékképeinket gazdagítják.

A digitális kor, amelyben élünk

A digitális korról számos tanulmány jelent meg, többek között Dyson (1998), Shapiro és Varian (1999), Kehal és Singh (2004), Barabási (2014) és Kollár (2011) szerzőktől. Bár a megközelítések és az elméletek nem feltétlenül kongruálnak egymással, néhány következtetés felsorolás jelleggel megfogalmazható a digitális korról:

– a külvilágban levő adatok folyamatosan digitalizálódnak (analóg-digitális átalakítás), majd

– további feldolgozásuk már digitális platformokon történik;

– az adatok feldolgozása során keletkezett információk, illetve a képzett tudás is rendszerint digitális platformokon tárolódik;

– a hagyományos javakhoz képest a digitális javak sokkal gyorsabban állíthatóak elő;

– előállítási költségük minimális, akár nulla közeli is lehet;

– a digitális javak gyorsan sokszorosíthatóak, vagy a technika eleve olyan, hogy „végtelen" nagy a példányszám, így akár vírusszerűen is terjedhetnek;

– behálózva éljük életünket, gyakorlatilag 24/7-es üzemben vagyunk online módban;

– az információ és az adat mint szellemi tulajdon új értelmezést kap;

– az információ gyorsan és relatíve kis költség mellett juttatható célba;

– az információ és az adat mint érték új értelmezést kap;

– felértékelődnek az adatok, az információk és a belőlük képzett tudás, egyre gyakrabban hallhatunk a vállalatok és az állami szervezetek adatvagyonáról;

– a digitális kor, vagy más névvel az adatok kora, másfajta gazdasági és társadalmi modellek szerint működik, mint az előző korok;

– az emberek és a vállalatok jelentős része nem méri fel kellő komolysággal az információbiztonság fontosságát.

A digitális kort számos technikával lehet jellemezni, a legfontosabbak a következők:

– *Cloud:* felhőalapú számítástechnika. Rögzített emlékeink jelentős része már gyakorlatilag felhőalapú tárhelyeken tárolódik. Rendszerint nem tudjuk, vagy legalábbis nem foglalkoztat minket, hogy az adatainkat tároló szerverek hol, a világ mely részén vannak, a lényeg, hogy adatainkat bárhonnan, bármilyen platformon (eszköz és operációs rendszer), bármikor el tudjuk érni, illetve bárhonnan, bármilyen platformról és bármikor újabb digitalizált emlékeket tudjunk rögzíteni és tárolni. Kevesen gon-

dolnak bele, hogy azzal, hogy a felhőben tárolják az adataikat, az azok feletti kontrollt vagy annak egy jelentős részét elveszítik, s amennyiben a felhőt informatikai támadás éri, az ott tárolt emlékek végképp elveszhetnek a számunkra.

– *Analytics:* nagy mennyiségű adatok gyors és szofisztikált elemzése. Az elemzés során egy személyről viszonylag kevés adat is elég ahhoz, hogy megrajzolható legyen megannyi algoritmus lefuttatása után egy közel teljes személyiségrajz. A hipotézisek helyét az adatbányászat és az algoritmizálás veszi át. Mivel ilyen nagy mennyiségű adatnál már szinte bármi között lehet találni kapcsolatot (korreláció), ezért jelenleg még az emberi intelligencia szükséges ahhoz, hogy az eredményeknek legyen köze a valósághoz, ne csak egy mesterséges intelligencián alapuló elburjánzott globális korrelációhalmazt kapjunk. Fényképeink, videóink, szövegeink, mások megjegyzéséhez fűzött megjegyzéseink, a digitális térben történő cselekvésünk, melyekből mind-mind emlékeink is lehetnek nemcsak a múltunkról és a jelenünkről, hanem egyre szofisztikáltabban a jövőnk számára is szolgáltatnak információt.

– *Mobile:* mobil- és hordozható eszközök (pl. okostelefonok, tabletek, laptopok) és mobilalkalmazások. A mobileszközökre – különösen az okostelefonokra – gyakran mint intelligens testrészre tekintünk, amelyik szerves és elválaszthatatlan része hivatalos és privát életünknek egyaránt. Nemcsak a kapcsolattartás és a webes böngészés során használjuk, hanem digitális krónikásként a segítségével adunk hírt, és rögzítjük digitális emlékként életünk megítélésünk szerint fontos eseményeit. A mobileszközeink elvesztése vagy feltörése során a rajta tárolt adatok elvesztése egyre többünk számára jelent visszafordíthatatlan katasztrófát (lásd később a szekunder kutatás bemutatásánál).

– *Social media:* közösségi média. A közösségi média, mint amilyen többek között a Facebook, a YouTube, a Twitter vagy a LinkedIn, alapfilozófiája szerint elsősorban a kapcsolattartásra, az ismerősök életeseményeinek a megismerésére, saját történéseink megosztására, valamint az online diskurzusok (pl. bejegyzés, válaszbejegyzés, mások bevonása a beszélgetésbe, lájkolás, megosztás stb.) számára kínál lehetőséget. A közösségi médiában található s sokak által látható emlékeink könnyen eshetnek áldozatul rossz szándékú egyéneknek és csoportoknak. Ez jelenti ugyanis a nem üzleti célú social engineeringgel foglalkozóknak az egyik legnagyobb „vadászati" terepet: személyiséglopás, személyiségklónozás, kapcsolati háló feltérképezése, megtévesztés, zaklatás – hogy csak a legfontosabbakat említsem.

– *IoT:* a dolgok internete. Az emberek által használt eszközök, ruhák, tárgyak, dolgok szenzorokat és aktuátorokat kapnak, illetve az internetre csatlakoznak. A szenzoroktól függően, közel valós időben és akár folyamatosan is lehet rögzíteni az emberben (pl. vérnyomásmérés, testhőmérséklet), illetve a környezetében zajló (fizikai) változásokat (pl. sebesség, páratartalom), majd ugyancsak közel valós időben lehet ezeket az adatokat továbbküldeni a különböző adatbázisokba és a felhőben levő adatelemző alkalmazásokra. Ezek közel valós időben azokat kielemzik, és összevetik más szenzorok eredményeivel, majd közel valós időben a felhasználót tájékoztatják a számára fontos kielemzett eredményekről. Azzal, hogy életünk folyása (pontosabban annak fizikai/kémiai/biológiai paraméterei) folyamatosan mérhetővé és elemezhetővé

válik, lehetővé teszi olyan emlékek elemzését is, amire korábban nem volt lehetőség, vagy sokkal kevesebb embernek adatott meg. Az adatok manipulálhatóak, az adatbázisok feltörhetőek, így a realitáson alapuló emlékeink közel valós időben módosulhatnak vagy törlődhetnek.

– *Robots:* robotok és drónok. Robotokat már több, drónokat pedig már közel egy évtizede használnak az iparban, a katonai és bizonyos polgári (pl. rendőrség) területeken. Az ezekre az eszközökre szerelt szenzorok, illetve hang- és képfelvételre és -rögzítésre használt berendezések révén az egyébként intim cselekedeteink (pl. naturista fürdőzés a feleségünkkel a saját kertünkben) könnyen mindenki által látható nyilvános performance-szá válhatnak.

A digitális kor előtt sokkal tudatosabban tudtuk eldönteni, s rendszerint magunk dönthettük el, hogy akarunk-e, s ha igen, milyen módon emléket rögzíteni az életünkből, s miután a rögzítés sikerült, azt kikkel s milyen módon szeretnénk megosztani. Nem azt állítom, hogy pl. a közösségi médiaoldalak nem biztosítanak bizonyos szabályozási/beállítási lehetőségeket rögzített emlékeink megtekintési jogosultságait illetően, de összességében a digitális kor sokkal jobban és mélyebben lépett be privát életünkbe, elmosva a határt a hivatali és a privát között, illetve gyakran tudtunkon kívül is betekintést engedve másoknak életünk intim részleteibe.

Megjegyzem, hogy a fenti felsorolást még illik kiegészíteni két területtel, a biztonsággal, illetve a kiterjesztett valósággal, melyekről, saját gondolatmenetem mentén, később kívánok írni.

Egy szekunder kutatás eredményei

A Kaspersky Lab 2015 júniusában tette nyilvánossá online, nagymintás primer kutatásának eredményeit. A 6000, brit, francia, német, olasz, spanyol és Benelux állampolgár részvételével zajló felmérésben – melyben 16 évnél idősebb nőket és férfiakat kérdeztek meg – a digitális amnézia elterjedését és hatását vizsgálták, vagyis azt, hogy a digitális korban az emberek mennyire hagyatkoznak az adatok előhívása és az emlékek felidézése során az eszközeikre, valamint arra is kíváncsiak voltak, hogy mennyire védik azokat az informatikai támadásokkal szemben. A digitális világban az amnézia a hagyományos megközelítés szerint egy olyan jelenség, amikor a tudás s így az emlékek végérvényesen elveszhetnek, ha az adathordozó médiát nem lehet olvasni, egyéb hardver-, illetve szoftverproblémák adódnak, s ezáltal a felejtés javíthatatlan és helyrehozhatatlan. A felmérésben arra keresték a választ, hogy mit tesznek az emberek, hogy csökkentsék a digitális amnézia kockázatát saját eszközeiken és alkalmazásaikon.

Kiderült, hogy a megkérdezettek 53%-a gyermekének, 90%-a gyermeke iskolájának, 51%-a munkahelyének, 33%-a partnerének, 40%-a pedig gyermekkori otthoni vonalas készülékének a telefonszámára már nem emlékszik. Ez olyan fokú függést jelent az okostelefontól, hogy ha három emberrel olyan baleset történne, amelyben nemcsak ő, hanem a telefonja is megsérül, közülük egy nem tudná felhívni a partnerét, hogy segítséget kérjen tőle, illetve nem tudná megadni a telefonszámát a mentősök-

nek sem, hogy felhívják őt. Az adatok elemzése során a kutatók megállapították, hogy az emberek egyre kevésbé képesek fontos információkat memorizálni, ahogy több válaszadó megjegyezte: nincs szükség az adatok memorizálására, arra ott az okostelefon. A 16 és 24 év közöttiek 43%-a szinte minden szükséges információt a telefonjában tárol, vagyis ha a telefonjukat elveszítik, vagy a készülék elromlik, akkor tízből négy fiatal végképp elveszíti a számára fontos információkat (pl. jelszavak, nevek, e-mail-címek, telefonszámok, szériaszámok, címek, névjegykártyák, kódok stb.). A nők, illetve az említett korosztály 40%-a mélységesen szomorú lenne, ha ez a végleges emlék- és adatvesztés megtörténne. A nők 25%-a végleges adatvesztéskor teljesen kétségbeesne, mivel ők emlékeiket és kapcsolati adataikat csak okostelefonon tárolják.

David Emm, a Kaspersky Lab senior biztonsági kutatója az eredmények alapján úgy gondolja, hogy egyre összetettebb világunkban az embernek túl sok számot, címet, nevet és egyéb adatot kell megjegyeznie, ami egyre nehezebb feladatot jelent a számára. A fentiek ismeretében úgy gondolhatnánk, hogy az információbiztonság kiemelt jelentőséggel bír az eszközhasználók számára. A kutatás eredményei azonban azt mutatják, hogy a megkérdezetteknek csak közel harmada telepít informatikai adatvédelmi szolgáltatást okostelefonjára, 23%-a tabletjára, s minden ötödik ember semmilyen módon nem védi eszközeit és a rajta található adatokat, információkat, emlékeket.

Emlékeink (információ)biztonsága

Az adatok, az adattárolók, a hálózatok, valamint az azokat használó személyek a digitális korban megannyi olyan támadásnak vannak kitéve, ami a social engineering, vagyis a pszichológiai manipuláció témakörébe sorolható. A social engineering technikák rendszerint két nagy területre oszthatóak (Oroszi, 2008): humán alapú, illetve számítógép-alapú social engineering technikák. A többnyire hackerek által megvalósított social engineering típusú támadások célpontjai általában a vállalatok, a kormányzati szervek, amelyek megtámadása üzleti haszonszerzés céljából, politikai indíttatásból vagy hírnév szerzése végett történik, de gyakorlásnak az átlagemberek is megfelelnek.

Emlékeink információbiztonságát érintő fontosabb események:

1. Az emlékeink lenyomatait tároló eszközök ellopása, elvesztése; eladása; kölcsönadása; szervizeltetése.

Javaslat: az eszközöket jelszóval lássuk el, a fontosabb emlékeinkről mindig legyen egy másolat egy másik eszközön vagy a felhőben, eladás előtt minden adatot töröljünk, lehetőleg ne adjuk kölcsön senkinek sem az eszközeinket, vagy ha igen, akkor előtte készítsünk biztonsági másolatot. A biztonsági másolat készítése igaz a szervizbe adásnál is.

2. Az adattárolók ellopása, elvesztése; kölcsönadása.

Javaslat: a fontos emlékeinkről mindig legyen biztonsági másolat egy másik eszközön vagy a felhőben. Ne vagy csak megbízható ismerősnek adjunk kölcsön adattárolót (pl. pendrive).

3. Személyes adatokkal és emlékekkel történő visszaélés.

Javaslat: nem kell életünk minden eseményét megosztani a közösségi oldalakon. A visszaélés kockázatát csökkenti, ha a közösségi média által kínált megosztási lehetőségek segítségével beállítjuk a megtekintési jogosultságokat.

4. Eszközök és a rajtuk futó alkalmazások feltörése.

Javaslat: ne adjuk kölcsön az eszközöket. Olyan jelszavakat használjunk, amelyek nem találhatóak ki könnyen (pl.: nem becenév, nem állat neve, de értelmetlen betű- és számsor javasolt). Minden lehetséges felkínálás ellenére se fogadjuk el a böngészők automatikus jelszómentési lehetőségét.

5. Eszközök vírussal történő megfertőzése.

Javaslat: ne adjuk kölcsön az eszközöket.

6. Eszközökről és/vagy távoli tárhelyekről (felhő) történő adat- és emléklopás.

Javaslat: mint a (4) pontban. A fontos adatokról és emlékekről egy másik eszközön, másik felhőben legyen biztonsági másolat. Nem kell mindenkinek tudnia, hogy milyen felhőalapú szolgáltatásokat veszünk igénybe.

7. Eszközökön és/vagy távoli tárhelyeken (felhő) történő adat- és emlékmódosítás.

Javaslat: mint a (6) pontban.

8. Eszközökön és/vagy távoli tárhelyeken (felhő) található adatok és emlékek végleges törlése.

Javaslat: mint a (6) pontban.

9. A látogatott weboldalak feltörése és/vagy elérhetetlenné tétele.

Ennek kivédése elsősorban nem az átlagember, hanem a tárhely-, illetve a tartalomszolgáltató felelőssége.

10. A weboldalakon található tartalmak hitelessége.

Ennek biztosítása elsősorban nem az átlagember, hanem a tartalomszolgáltató felelőssége. A hitelesség vizsgálata azonban már az átlagemberre is tartozik. Korábban az „olvastam az újságban", „láttam a tévében", mostanság pedig „olvastam/láttam az interneten" kezdetű mondatokkal szeretnének állításaiknak igazolást nyerni az átlagemberek. Számos zombimédium erre építve folyamatosan ontja magából a hamis, megalapozatlan (rém)híreket.

11. A weboldalakon található tartalmak illetéktelen módosítása.

Ennek kivédése és ellenőrzése elsősorban a tárhely-, illetve a tartalomszolgáltató felelőssége. A probléma az, hogy a jól megvalósított tartalommódosítás (emlékátírás) nagyon nehezen vehető észre (bár, ahogy korábban utaltam rá, van lehetőség az esetek egy részében a módosítás előtti változatok megtekintésére), de egy átlagos felhasználónak sem kedve, sem ideje nincs arra, hogy minden tényadatnál és emléknél ellenőrizze, hogy azt módosították-e. De ha ezt meg is teszi, akkor sem tudhatja, hogy a módosítás révén objektívebb és teljesebb adatok állnak a rendelkezésére, vagy csak egy illetéktelenül kozmetikázott, hamis emlékkép.

12. A polgárok adatait tartalmazó adatbázisok feltörése, s onnan az adatok és emlékek ellopása

Ennek kivédése elsősorban nem az átlagember, hanem a tárhely-, a tartalomszolgáltató, valamint az adatbázis üzemeltetőjének a felelőssége. A javaslat megegyezik a (6) pontban leírtakkal.

13. Ransomware.

Emlékeink túszok lettek. Viszonylag új jelenségnek számít (bár a gyökerek 1989-ig nyúlnak vissza), hogy a digitális eszközeinken tárolt adatainkat és emlékeinket egy vírus vagy maga a támadó nem törli le, s nem is módosítja azok tartalmát. Helyette blokkolja a hozzáférést a számítógéphez, illetve a fájlokhoz. A támadó pénzt akar kizsarolni az áldozattól, s csak ennek megérkezése után hajlandó a blokkolást feloldó kódot elküldeni.

Javaslat: semmilyen gyanús csatolmányt ne nyissunk meg (gyanúsnak számít pl. ismeretlen feladó, vagy a feladó ismert, de nem fűz a csatolmányhoz semmilyen értelmes megjegyzést). Lehetőleg legális forrásból származó szoftvereket használjunk (tehát nem feltört Windowst vagy SPSS-t). Legyen a számítástechnikai eszközeinken vírusirtó, s ha figyelmeztet egy gyanús fájlra, akkor győzzük le a kíváncsiságunkat, s ne nyissuk meg. Ne torrentezzünk, vagy ha mégis ezt tesszük, járjunk el kellő gondossággal és körültekintéssel.

Következtetések és jövőkép

A biztonság mellett a kiterjesztett valóságról is említést kell tenni. A *kiterjesztett valóság* (augmented reality) a kevert valóságok sorában a fizikai valóság és a virtuális valóság között helyezkedik el. A látható, fizikai, kézzelfogható valóság a számítógéppel generált elemekkel egészül ki, s így ez a kiterjesztett valóság válik a felhasználó számára elérhetővé (Kollár, 2012). A kiterjesztett és a virtuális valóság közötti lényeges – technikai – különbség az, hogy az előbbinél a fizikai és a mesterséges világ együtt jelenik meg, míg az utóbbinál a fejünkre húzott VV- (virtuális valóság) sisak révén csak a mesterséges világ. Pszichológusok és médiaszociológusok már a film korában is értekeztek arról, hogy a filmeken látott fiktív világ keveredhet az emberek emlékezetében a fizikai világgal, s akár az utóbbi rovására hamis emlékképekkel gazdagodik emléktárunk. A digitális technikák – mint amilyen a kiterjesztett és a virtuális valóság is – elterjedése és megjelenése az emberek életében azonban sokkal markánsabban képes hatást gyakorolni rájuk. A HVG biztonságról szóló számában Bari (2016) több kutatás eredményét összegzi:

– Keck Center for Neurophysics: patkányokat virtuális valóságba helyeztek. A vizsgált neuronok 60%-a kikapcsolt. A nem kikapcsolt idegsejtek abnormális működést mutattak.

– Lee Hutchinson (Ars Technica): a VR használatakor a pixelrács beégett a látómezőbe, sokáig szellemképesen látta a használatát követően.

– Albert Rizzo (Dél-kaliforniai Egyetem): kéz-szem koordinációs problémák (túlnyúlás) jelentkezhetnek.

– GTP (game transfer phenomena) jelensége: a játékok elemei (képek, hangok, személyek) átszivárognak a valóságba, a játékosok úgy reagálnak a valós világban, mint a virtuálisban.

– Hamburgi Egyetem: 24 órás VR-kísérlet: a tesztalanyok összekeverték a valós és a virtuális valóságot – mind az élményeket, mind a tárgyakat.

– Andrew Doan (USA Navy): a virtuális valóság izgalmasabb agyunknak az igazinál, ezért egyre nagyobb függőségek alakulhatnak majd ki.

Bari meglátása szerint nem fogjuk tudni, hogy az egyes emlékek mely valóságból származnak.

Nem jelenthet igazi megoldást az sem, ha a kiterjesztett, illetve különösen a virtuális valóságot kizárjuk az életünkből. A Google effects (Sparrow–Liu–Wegner, 2011) – vagy egyes teoretikusok véleménye szerint azzal szinonim fogalomként a digitális amnézia – néven ismert jelenség lényege, hogy a Google és más keresők egyre kifinomultabb keresési algoritmusai révén egyre többen hagyatkoznak a keresőre, bármilyen információra is van szükségük, ahelyett hogy magát az információt jegyeznék meg. Nem kell ugyanis nagy erőfeszítéseket tenni annak érdekében, hogy az emberek megtalálják azt, ami érdekli őket. Sőt, bizonyára sokunknak az is feltűnt már, hogy miközben a Google keresősorában elkezdünk begépelni valamit, nagy valószínűség szerint már előre kitalálja, hogy mit akarunk, s megjeleníti a teljes szót, illetve keresőkifejezést. A Google az interneten található tartalmakra hagyatkozik a keresés közben, s pont emiatt mondhatjuk azt, hogy az internet lett az elsődleges formája a külső vagy tranzaktív memóriának. Hivatkozott szerzők kutatási eredményei is megerősítik, hogy az emberek már elsősorban azt jegyzik meg, hogy az információt hol keressék, nem pedig magát az információt.

Zárógondolatok

A digitális tartalmak vírusszerű terjedési lehetősége, a kollaboratív szűrés (amilyen tartalmakat korábban néztünk, ahhoz hasonlók jelennek meg) alkalmazása valamennyi olyan helyen, ahol a felhasználót azonosították, ahhoz a szomorú felismeréshez vezet, hogy a médiafogyasztókat egy olyan tölcsérbe vezetik bele, amely egyre mélyebbre és mélyebbre viszi őket az adott téma mentén. A tölcsér falán pedig megjelennek azok az emlékek, amelyekre visszanézve már nem is vizsgáljuk meg, hogy valósak-e, vagy sem, egyszerűen elfogadjuk azokat olyannak, amilyenek.

E felismerés alapján fogalmazódik meg bennem a zárókérdés: fontos-e az emlékezés? Ha identitásunkat vizsgáljuk, akkor azt mondhatjuk, hogy igen. Ha nem tudunk emlékezni, vagy hamis emlékeink vannak, akkor az utunk s így a jövőnk is bizonytalanná, hamissá s külső erők által irányítottá válik. Ez persze lehet egyfajta cél is, de a többség számára nem kecsegtet semmi jóval. Emlékeink információbiztonsága és megbízhatósága pont a jól látható és tervezhető jövő miatt bír kiemelt jelentőséggel.

Felhasznált irodalom

Barabási, Albert László (2014): *Linked. How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life.* Basic Books, New York.

Bari Máriusz (2016): Ember egy másik világban. *HVG Extra Business,* 1. sz., HVG, Budapest.

Dyson, Esther (1998): *Release 2.0.* Broadway, London.

Féjja Sándor (1982): *Tizenöt filmlecke.* Műszaki Könyvkiadó, Budapest.

Hewitt, William W. (2008): *Hipnózis kezdőknek. A tudatosság és az önmegvalósítás új szintjei.* Alexandra Kiadó, Budapest.

Index (2013): Leleplezték a Wikipedia legnagyobb átverését. *Index.hu,* http://index.hu/tech/2013/05/01/lelepleztek_a_wikipedia_legnagyobb_atvereset/.

Kaspersky Lab (2015): *The Rise and Impact of Digital Amnesia.* Kutatási jelentés.

Kehal, Harbhajan – Singh, Varinder P. (2004): *Digital Economy. Impacts, Influences and Challenges.* Idea Group Publishing, London, https://doi.org/10.4018/978-1-59140-363-0.

Kollár Csaba (2011): Digitális nemzedékek Magyarországon és külföldön. In: *Vállalati kommunikáció a 21. század elején.* Szerk. Borgulya Ágnes, Deák Csaba, Z-Press Kiadó, Miskolc.

Kollár Csaba (2012): A kiterjesztett valóság (Augmented Reality) (nem csak) üzleti és marketinges lehetőségei. In: *A filozófia párbeszéde a tudományokkal. A 70 éves Tóth Tamás professzor köszöntése.* Szerk. Farkas Attila, Kollár Csaba, Laurinyecz Ágnes, Protokollár Tanácsadó Iroda, Budapest.

Levinson, Jay Conrad – McLaughlin, Michael W. (2005): *Guerrilla Marketing for Consultants. Breakthrough Tactics for Winning Profitable Clients.* John Wiley & Sons, New Jersey.

Lukacs, John (2012): *A történetírás jövője.* Európa Könyvkiadó, Budapest.

Newman, Bruce I. (2000): *Politikai marketing mint kampánystratégia.* Bagolyvár, Budapest.

Oroszi Eszter Diána (2008): *Social Engineering. Az emberi erőforrás, mint az információbiztonság kritikus tényezője.* BCE, Budapest.

Pinker, Steven (2002): *Hogyan működik az elme.* Osiris Kiadó, Budapest.

Purkins, John – Royston-Lee, David (2010): *Énmárka. Tedd magad eladhatóvá!* HVG Könyvek, Budapest.

Schawbel, Dan (2012): *Én 2.0. Építsd online a személyes márkád!* HVG Könyvek, Budapest.

Shapiro, Carl – Varian, Hal R. (1999): *Information Rules. A Strategic Guide to the Network Economy.* Harvard Business School Press, Boston.

Sparrow, Betsy – Liu, Jenny – Wegner, Daniel M. (2011): Google Effects on Memory. Cognitive Consequences of Having Information at Our Fingertips. *Science,* Vol. 333, No. 6043, 776–778, https://doi.org/10.1126/science.1207745.