Kollár Csaba

Az információbiztonság időszerű kérdései.

Az európai Z generáció oktatása a digitális korban

Az Európai Unióról, valamint működéséről szóló szerződés, illetve az Alapjogi Charta értelmében mindenkinek joga van az oktatáshoz. E jog érvényesítése érdekében biztosítani kell az oktatáshoz való széles körű hozzáférést, az ismeretek folyamatos frissítését, a távoktatás fejlesztését. Nevezett dokumentumok kimondják továbbá, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez, értve ezen a róla szóló szöveges tartalommal, őt ábrázoló képekkel, videókkal kapcsolatos önrendelkezési jogot, saját (virtuális) személyiségének a védelmét, az általa előállított s más személyiségi és egyéb jogait nem sértő tartalmak szabad kezelését (pl. törlés, módosítás, megosztás). Az Európai Unió dokumentumai, illetve azok értelmezései megfelelő keretet adnak a tanulmányom fókuszában levő Z generáció oktatásának és az információbiztonság kapcsolatának a vizsgálatához. A tágan értelmezett távoktatás módszertanában megnevezett digitális platformok használata a Z generáció számára a napi rutin része (Kollár, 2014a), míg az őt oktató idősebb generáció tagjainak tanult cselekvés, hiszen a Z generáció már születése óta a digitális platformokon keresztül közvetített tartalmak révén is, sőt markánsan azáltal szocializálódott. A digitális javakhoz történő könnyű, gyakran meggondolatlan hozzáférés azonban információbiztonsági szempontból is számos veszélyt jelent. Tanulmányom utolsó részében e veszélyeket, illetve csökkentésük lehetséges módszereit mutatom be.

Az EU 28 tagállamának generációi a statisztikák tükrében

Az Eurostat 2015. január 1-jére vonatkozó demográfiai statisztikái szerint a Z generációsok, vagyis az 1996 és 2009 között születettek, az EU 28 tagállama összlakosságának a 14,71%-át teszik ki közel 75 milliós lélekszámukban. A Z, valamint a többi generáció létszámát, illetve százalékos arányát az 1. táblázat szemlélteti.

1. táblázat: Az EU 28 tagállamának generációi (Eurostat 2015 alapján saját szerkesztés)

Generációk[1]	születési idő		életkor		nemek [millió fő]		nemek [%]		Összesen [millió fő]	összesen [%]
	-tól	-ig	min.	max.	férfi	nő	férfi	nő		
veteránok (70+)		1945	70		27,92	40,40	41%	59%	68,31	13,44%
babyboom	1946	1964	51	69	58,96	62,75	48%	52%	121,71	23,94%
X	1965	1979	36	50	54,89	54,66	50%	50%	109,55	21,55%
Y	1980	1995	20	35	51,84	50,62	51%	49%	102,46	20,15%
Z	1996	2009	6	19	38,39	36,42	51%	49%	74,81	14,71%
alfa	2010			5	16,21	15,39	51%	49%	31,60	6,22%
Összesen:					**248,21**	**260,24**	**47,60%**	**52,40%**	**508,45**	100%

Az 1. táblázat alapján megállapíthatjuk, hogy életkoruk szerint döntő többségében a babyboom, az X, illetve az Y generáció tagjai vannak jelen a munkaerőpiacon. Ez több dolgot is jelent a 28 európai országban élő Z generáció vonatkozásában:

1. Elsősorban ezek azok a generációk, amelyek a Z generációs fiatalok hagyományos oktatásában részt vesznek, értve ezen a tanítás mellett a tananyagok fejlesztését, a könyvek/jegyzetek írását, valamint a generáció-specifikus oktatástechnikai eszközökre, alkalmazásokra és platformokra épülő – elméletileg – interaktív, lebilincselő, informatív, modern tartalmak ellőállítását is.

2. A hagyományos(nak mondott) médiatartalmak (TV, rádió, újság) jelentős, az új médiában (internet) megjelenő tartalmaknak pedig egyre kisebb részét állítják elő a nem Z generációsok. Különösen igaz ez az általuk egyre kevésbé értett WEB 2.0 platformokra.

3. Ezek azok a generációk, amelyek most, illetve néhány éven belül kollégákként, munkatársakként találkoznak a Z generációsokkal, s egyre valószínűbb, hogy saját munkaszocializációs emlékeiket nem tudják feszültségmentesen alkalmazni erre a generációra.

4. A vállalatok vezetői és tulajdonosai jelenleg rendszerint nem Z generációsok, de ahhoz, hogy a megannyi, s egyre újabb technikai eszközökkel/alkalmazásokkal/platformokkal átszőtt digitális korba beleszületett Z s az őket követő alfa generáció fogyasztói igényeinek meg tudjanak felelni, szükségszerűen rákényszerülnek arra, hogy megtanulják az Európai Unió jövőbeli aktív és önmegvalósító fogyasztóinak (Z+alfa hozzávetőlegesen 106 millió fő) a speciális nyelvezetét.

5. Miközben a nem Z generációsok nagyobb bölcsességgel, munkatapasztalattal rendelkeznek, s többségük megfontoltabb és távolságtartóbb, addig a Z generációsok – életkorukból is adódóan – sokkal lazábbak, könnyebben létesítenek és tartanak fenn (felszínes) emberi kapcsolatokat, s így sokkal könnyebben lehetnek áldozatai az idősebb

bűnelkövetői csoportoknak (pl.: személyes adataikkal visszaélés, pedofília, érzelmi zsarolás, érzelmi függés – lásd később).

Az Európai Unió generációinak, a munka világa és a digitális eszközökkel történő első találkozását foglalja össze a 2. táblázat.

2. táblázat: Az Európai Unió generációi a munka világában, s találkozásuk a digitális eszközökkel (saját szerkesztés)

Generációk	**Munka**	**Találkozás a digitális eszközökkel**
veteránok (70+)	rendszerint nyugdíjasok	életük második felében találkoztak az internettel
babyboom	fontos hányadát teszik ki a munkaerőpiacnak, egy részük már nyugdíjba készül	30–40 éves koruk körül
X	a munkaerőpiac gerince	kamaszként, tinédzserként
Y	tanulók, vagy néhány éves tapasztalattal rendelkeznek a munkaerőpiacon	gyermekkorban
Z	tanulók, vagy kis részük pályakezdő	nem éltek az internet világa nélkül
alfa	-	nem éltek a mobilinternet nélkül

Lehetőségem volt a tanulmány megírását megelőzően egy viszonylag egyszerű felmérést végezni egyik egyetemi munkahelyemen (SZIE GTK). Néhány kollégámnak és hallgatóink egy részének egy új, számukra még ismeretlen eszközt (IoT) mutattam meg, s kíváncsi voltam a reakcióikra (módszertan: Horváth és Mitev, 2015). Íme a fontosabb megállapítások generációnként:

1. Babyboom (kollégák): nem szívesen vették kézbe, idegenkedtek tőle. Tőlem várták a választ a használatot illetően. Mikor elmondtam, hogy ezt a tantárgyak oktatásában is fel lehet használni, akkor rendszerint írásos anyagot kértek tőlem, ami részletesen elmagyarázza az eszköz használatát, illetve volt, aki megkérdezte, hogy tartunk-e egy rövid felkészítőt.

2. X (kollégák): némi bátorítás után kézbe vették. A használatot illetően egy részük nyomtatott anyagot kért, míg egy másik részüknek elég volt, ha elküldöm pdf-ben a részletes használati útmutatót (majd ő, ha kell, kinyomtatja magának).

3. Y (nappali és levelező tagozatos hallgatók, kollégák): szinte azonnal kézbe vették. Kivétel nélkül megelégedtek az elektronikus ismertetőkkel, ami lehetett egy link, ahonnan le lehet tölteni pdf-ben egy rövid (!) ismertetőt, vagy egy Youtube videó, ami röviden bemutatja a használatot.

4. Z (nappali tagozatos hallgatók): azonnal kézbe vették, s mikor elmondtam a nevét és egy mondatban, hogy mire jó, máris gépelték be azt az okostelefonjukba. Gyakorlatilag elég volt nekik egy impulzus, ami felkeltette az érdeklődésüket, a továbbiakban már nem szorultak az én segítségemre.

Ez az egyszerű, jelzés értékű felmérés is megerősíti azt a képet, hogy a digitális korban különösen a fiatalabb korosztályok/generációk számára már nem szükséges az információ materiális (kinyomtatott) megjelenése, elég, ha a laptop/tablet/okostelefon kijelzőjén keresztül el tudják érni a kívánt és számukra releváns tartalmakat. Ez azt is jelenti, hogy az EU távoktatásra vonatkozó elképzelései a fiatalabb generációk vonatkozásában társadalmilag is megalapozottak. Ugyanakkor azt is látni kell, hogy a Z, majd az őket követő alfa generációsoknak csökken az igényük az adott dolog részletes, minden területre kiterjedő megismerésére, rendszerint elégségesnek tartják, ha a cél sikeres eléréséhez szükséges mértékben tudják használni a megszerzett információkat.

A Z generáció

A Z generációba tartozó fiatalok – ahogy már arra többször is utaltam – 1996 és 2009 között születtek, pontosabban beleszülettek a digitális technológiák világába (digitális bennszülöttek) (Kollár, 2011b). Mindennapi tevékenységeik során a digitális eszközök használata a napi rutin részévé vált. A mobiltelefonra mint leválaszthatatlan „testrészre" gondolnak, s rendszerint karnyújtásnyi távolságon belül szinte bármikor el tudják azt érni. Többségük úgy gondolja, hogy a világ csak akkor forog, s benne csak akkor tartalmas az életük, ha annak minden rezdüléséről posztolnak. Ahogy egyikük kifejtette a véleményét az egyik Facebook posztjában: „én csak akkor vagyok valaki, ha megosztom az életemet" (a digitális platformokon). Miközben a digitális környezetben viszonylag könnyen találják meg a helyüket, addig a fizikai világban egy számottevő részük beilleszkedési gondokkal küzd. Talán ennek is köszönhető, hogy egyre több tevékenységet (pl. tanulás, kapcsolatépítés és -tartás, találkozások) már digitális platformokon végeznek (Kollár, 2011a). A strukturált tanulás helyett a véletlenszerű megismerést tartják elfogadhatónak, a vaskos könyvek és a klasszikus lexikális tudás helyét átveszik náluk a Youtube és más videomegosztó oldalak rövid videói. Kevesebbet olvasnak, sokkal többet játszanak, s ennek is köszönhető, hogy az ismeretátadás új formáit kell keresniük a reformpedagógusoknak (pl.: gamification, edutainment). A hagyományos oktatást lassúnak és unalmasnak találják. Ahogy a korábbi generációknak a könyv, az újság, majd a TV/rádió jelentette a „megkérdőjelezhetetlen" forrást, addig a Z generáció számára az internet az. Ez számos információbiztonsági kérdést is felvet, hiszen míg a könyv, az újság, a rádió és TV tartalmának előállítása (elvben) felelősségteljes és kontrollált (pl. felelős szerkesztő, kiadó) folyamat volt, ezzel biztosítva az objektív és tárgyilagos közlést, addig a neten gyakorlatilag egy egyszerű mobiltelefonnal felvett videotartalom is hamar népszerűvé és véleményformálóvá válhat úgy, hogy a közölt információ valódiságát gyakran senki nem vizsgálja. A kevés élettapasztalattal rendelkező Z generáció így sokkal sebezhetőbbé és befolyásolhatóbbá válik.

Az idősebb generációk rendszerint szisztematikus sorrendet követve dolgozzák fel az információt, míg a Z generációsok inkább párhuzamosan. Ez egyfelől versenyképesebbé teszi őket, mivel hamarabb tudnak végezni a feladattal, de sebezhetőbbé is, hiszen a dömpingszerűen érkező információk párhuzamos feldolgozása során nincs idő azok

tényleges megkérdőjelezésére, ellenőrzésére, a köztük levő összefüggések vizsgálatára, megtalálására.

A Z generációsok ugyan életkorukból adódóan is zömében iskolások, de az életükhöz, boldogulásukhoz szükséges információ jelentős részét már nem az iskolából szerzik. A tudást egymás között osztják meg, s nem is tudástranszferként tekintenek ezekre a megosztásokra, sokkal inkább egyszerű haveri/baráti beszélgetésekre, ahol véletlenszerűen néhány ilyen téma is szóba esik.

A fentiek alapján azonban téves lenne azt következtetni, hogy a Z generációsok nem tájékozottak a nagyvilág dolgaiban. De miközben az idősebb generációkat (különösen a tanultabbakat) a hagyományosan megszerzett tudás köré épített információéhség motiválja (pl. politika, történelem, történelmi személyiségek, apa- és nagyapakorú zenészek és zenekarok), addig a Z generációsok számára fiatalságuk okán is sokkal fontosabb, hogy az aktuális popsztár mit csinált tegnap, hol s kivel volt. A Z generációsok számára is fontos, hogy kötődjenek bizonyos „objektumokhoz" (pl. tiniceleb), s emiatt ugyancsak sebezhetővé válnak (pl. pedofilok az adott celeb fényképével és nevével egy hamis Facebook oldalt hoznak létre, ahol a celeb nevében nagyon könnyen tudnak rábírni tinilányokat, hogy elmenjenek egy találkozóra is).

A Z generáció tanítói

Médiapedagógusok és az oktatástechnikával és -technológiával foglalkozó szakemberek véleménye jelentősen eltér arról, hogy ki tanítja a Z generációt. Rendszerint a következő személyeket/platformokat szokták megnevezni:

1. tanítók, tanárok, szaktanárok, egyetemi oktatók (fizikai világ);
2. saját nemzedéke, néhány évvel idősebb testvére (fizikai világ);
3. saját nemzedéke (digitális platformok);
4. az általa használt – zömében – WEB 2.0 alkalmazások és szolgáltatások (digitális platformok)

3. táblázat A Z generáció tanítói (saját szerkesztés)

Jellemzők	Fizikai világ		**Digitális platformok**	
	tanítók, tanárok, szaktanárok, egyetemi oktatók	**saját nemzedéke, néhány évvel idősebb testvére**	**saját nemzedéke**	**WEB 2.0 alkalmazások és platformok**
Tudás átadása	tanóra, szakkör, klub, tematika, tankönyv, jegyzet	leülünk tanulni, közös tanulás megmutatom neked	csevegés, fórumok	fórumok, Youtube, a google a te barátod

Jellemzők	Fizikai világ		Digitális platformok	
	tanítók, tanárok, szaktanárok, egyetemi oktatók	**saját nemzedéke, néhány évvel idősebb testvére**	**saját nemzedéke**	**WEB 2.0 alkalmazások és platformok**
Számonkérés módja	vizsga, szóbeli, ZH, házi dolgozat, szóbeli, írásbeli, témazáró, szigorlat, államvizsga, képesítő vizsga	én elmagyarázom neked, te visszamondod nekem, nincs számonkérés	nincs számonkérés	
Mit kérnek számon?	tények, adatok, összefüggések, minél több információ	gyakorlatilag semmit tudod használni? – nem kérdés, hanem a gyakorlatban bizonyítod		
Generáció	babyboom, X, Y digitális bevándorló	Z digitális bennszülött		Z (mögötte állhat X, Y)
Mottó	A tudásért meg kell dolgozni, én is megdolgoztam érte.	Szabadság, azt csinálok, amit akarok. azt posztolok, amit akarok.		

A Z generáció – információbiztonság a digitális korban

Az információbiztonság kapcsán három lényeges fogalmi alapvetés szükséges: 1. információs társadalom, 2. digitális kor, 3. információbiztonság.

Azzal mindannyian egyetérthetünk, hogy az ipari társadalom utáni korszakot hívják az *információs társadalom* korának. Az információs társadalom fogalmát azonban gyakran szinonim jelleggel a posztindusztriális társdalom, a posztfordizmus, a posztmodern társadalom, a tudástársadalom, a hálózati társadalom fogalmaival is helyettesítik.

Az információ és a tudás az információs társadalomban kiemelt jelentőséggel bír. Az információ kapcsán említést érdemelnek az alábbiak:

- az információ előállítása;
- az információ továbbítása;
- az információ tárolása;
- információ megszerzése;
- az információ értéke;
- az információ biztonsága (információbiztonság);
- az információ értékének időbeli változása;
- az információ sokszorozhatósása;
- az információhoz fűződő jog;
- az információszolgáltatási kötelezettség.

Az információ alapja mindig az *adat*. Az adat egy meghatározott dolog egy meghatározott változójának (karakter, attribútum, jellemző, tulajdonság, ismérv stb.) az értéke. Az adatok lehetnek: 1. nominálisak (pl. nem, név, törzsszám), 2. ordinálisak (pl. iskolai végzettség), 3. intervallumskálájúak (pl. hőmérséklet), 4. arányskálájúak (pl. a je-

lenlegi és a kezdőfizetés) (Ketskeméty, Izsó és Tóth, 2011). Összefoglalva azt mondhatjuk, hogy az információ olyan értelmezett adat, amelyikből valamilyen konkrét tényt tudhatunk meg. Az adatok régebben papíralapon (pl. személyügyi akta, személyi karton/nyilvántartó lap), az utóbbi időben azonban már rendszerint elektronikus, digitális úton tárolódnak (pl. adatbázisokban). Tévedés lenne azt hinni, hogy az *információ fogalma* csak a technikai eszközök megjelenésével vált ismertté. Latin eredetijében értesülést, hírt, üzenetet, tájékoztatást jelent, s általában úgy tekintünk rá, hogy akkor válik fontossá a számunkra, ha csökkenti az információhiányunkat, a bizonytalanságunkat. Az információ tehát eredeti – s általunk is használt – megközelítésében független a technikai eszközöktől, ugyanakkor a technikai és informatikai eszközök tömeges elterjedése tette lehetővé azt, hogy felértékelődjön. Az információ modern értelmezése kitér arra is, hogy elsősorban nem is az információ a fontos, hiszen szinte majd' minden területen információs többlet van, hanem az, hogy a rendelkezésünkre álló vagy viszonylag kis energiabefektetés révén megszerezhető információ hogyan, milyen módszerekkel, mennyi idő alatt és milyen hatékonysággal alakítható át, illetve dolgozható fel tudássá.

Az adatokból előálló információ s az információk feldolgozása során keletkező tudás számtalan (algoritmizált) számítást, komoly tárhely- és számítási kapacitást kíván meg. Ezeknek az elvárásoknak viszonylag könnyen meg lehet felelni úgy, ha minél hamarabb kerülnek digitális vagy digitalizált formába az adatok. A digitalizált adatokból számsorozatok lesznek, s így számítások milliói végezhetők el velük/rajtuk. A fizikai, szabad szemmel látható, illetve egyéb érzékszerveinkkel érzékelhető, valamint a nem látható, de paraméterei alapján mérhető világ végtelen adatmennyiséggel szolgál, s ezek egyre nagyobb hányada már digitális formában rögzül. A világ tehát egyre nagyobb mértékben „képződik le" digitális formában, s ezért mondhatjuk azt, hogy az információs társadalom/kor után a *digitális kor* következik (Kollár, 2014b). A digitális kor a XXI. század első évtizedétől számítható, bár előzményeiről már korábban is írtak (Dyson, 1997), de az alapművek később jelentek meg (Saphiro és Varian, 1999, illetve Levine és munkatársai (2001) (Levine, Locke, Searls és Weinberger, 2001), Kehal és Singh, 2004, Lessig, 2004, Wallace, 2002). A digitális kor dimenzióit egy rendszerint változó tartalmú mozaikszóval (CAMSSAIR) lehet leírni, mely jelenleg hangsúlyosan az alábbi elemeket tartalmazza:

– cloud: felhő, felhő alapú szolgáltatások;
– analytics: elemzés, adatbányászat;
– mobile: mobileszközök, mobilalkalmazások;
– socialmedia: közösségi média;
– security: biztonság;
– AR (augmented reality): kiterjesztett valóság (Kollár, 2012);
– IoT: internet of things;
– robots: robotok.

Információbiztonság

A digitális kor informatikai hátterének teljes bemutatása jelentősen túlmutat jelen tanulmány tartalmi és terjedelmi keretén, ezért az alábbiakban csak az információbiz-

tonság Z generációt érintő kérdéseivel foglalkozom. A digitális kor és a társadalom jövője szempontjából kiemelt jelentőséggel bír a biztonság (Security), s azon belül az információbiztonság. *Haig* (2015) is osztja *Gábri* (2008) véleményét, miszerint az információbiztonság az alábbi öt területet integrálja magába: politikai biztonság; társadalmi biztonság; gazdasági biztonság; katonai biztonság; környezeti biztonság.

Az információbiztonság nem csak informatikai kérdés, hiszen a műszaki-informatikai megoldások jelentős része az informatikai (IT) biztonság területéhez tartozik, sokkal inkább humán aspektussal bír. 2015 novemberében egy Európai Uniós fiatalok bevonásával megvalósuló projekt keretében én is meghívást kaptam, hogy egy rendhagyó osztályfőnöki órát tartsak az információbiztonságról. Az interaktív beszélgetés során elhangzott fontosabb problémákat s az azokra tett javaslatokat strukturált formában az alábbiakban adom közre. Az információbiztonság és veszély a Z generáció számára rendszerint a következőket jelentheti *Gyaraki* (2015), *Mitnick és Simon* (2006), *Schneier* (2010), *Warren és Streeter* (2005), valamint *Nábrády* (2014) munkái alapján:

1. A fiatalok által használt eszközök ellopása, elvesztése, eladása, kölcsönadása, szervizeltetése

a. Az eszközök ellopása, elvesztése során az azokon található tartalmak, illetve az azokon történő bejelentkezés során a távoli tárhelyeken tárolt tartalmak is elérhetőek illetéktelen személyek számára.

Megoldási lehetőségek:

– Az eszközökre történő belépés csak jelszóval lehetséges –, bár az elvesztés és ellopás során van ideje a tolvajnak/megtalálónak az eszközt szétszedve hozzáférni az adattárolókhoz (pl. SD kártya, winchester).

– Ha már elveszett, s fontos adatok vannak rajta, akkor meg lehet próbálni, hogy az adott személy visszavásárolja legalább az adattárolót. Kérdéses, hogy sikerül-e a „becsületes" megtalálót a közösségi háló segítségével megtalálni, s ha sikerül, akkor ő hajlandó-e, s ha igen, akkor milyen feltételek mellett. Ilyen esetekben célszerű felnőtt/szülő bevonása is.

– Ha a tettes ismert, azonnal meg kell tenni a büntetőfeljelentést.

b. Az eladásra ítélt készülékek megfelelő adatmentesítésével gyakran még a cégek sem foglalkoznak, s ez sajnos hatványozottan igaz a fiatalokra. A megunt okostelefonon szinte azonnal túl akarnak adni, hogy megvehessék a legújabb modellt.

Megoldási lehetőség: A fiatalok figyelmét felhívni az adatmentés és -törlés fontosságára, valamint arra, hogy a telefonon/készüléken állítsák vissza úgy a gyári beállításokat, hogy azzal az eszközön minden beállítás (belépési adatok, kedvenc oldalak) törlődjön.

c. A kölcsönadás és szervizelés során a fiatal egy megítélése szerint megbízható személynek vagy cégnek adja oda egy bizonyos időre a készüléket. A kölcsönadás sok esetben a barátság vagy éppen a közösséghez való tartozás, illetve az önzetlenség fokmérője is lehet.

Megoldási lehetőségek:

– Megértetni a fiatalokkal, hogy a személyes adataikat is tartalmazó eszközök kölcsönadása nem lehet semmilyen pozitív emberi érték fokmérője.

– A névtelen, nem megbízható szervizeket (pl. nincs igazi szerviz, a műszerésszel a mekiben lehet csak találkozni) még akkor is célszerű elkerülni, ha azok olcsóbbak, mint a hivatalos szervizek.

– Ha egy készüléket beadnak javításra a szervizbe, akkor arról előtte érdemes lementeni és utána letörölni a személyes adatokat, s a belépési jelszavakat ideiglenesen meg kell változtatni. A készülék javításra történő átvételét a szerviznek hivatalos átvételi bizonylattal kell elismernie.

2. A fiatalok által használt adattároló elvesztése, kölcsönadása

Megoldási lehetőségek: mint az 1. pontban.

3. A fiatalok interneten található személyes adataival történő visszaélés

A visszaélés lehet egy bizalmas, intim fénykép nyilvános megosztása, vagy egy profilkép és néhány egyéb adat ismeretében egy hamis felhasználói profil létrehozása. Egy ilyen hamis profil – mely gyakran egy egyszerű kamaszcsínynek tűnhet – alkalmas lehet arra, hogy a gyanútlan fiatalról hosszabb távra is hamis képet építsen, a nevében mindenféle nemkívánatos oldalra regisztráljon, ott véleményt fejezzen ki. Mivel a digitális lábnyom a szervereken és a logfájlokban akkor is megmarad, ha az adatok már nyilvánosan nem elérhetőek, így gyakorlatilag egy életre megmarad ez a hendikep.

Megoldási lehetőségek:

– A fiatal körültekintően jár el, s megtiltja, hogy róla kompromittáló kép készüljön, még akkor is, ha ezzel nem lesz népszerű a barátai, haverjai előtt.

– Amint tudomást szerez, hogy visszaéltek személyes adataival, azonnal szól szüleinek, akik hivatalosan megteszik a feljelentést a rendőrségen.

4. A fiatal által használt eszközök (okostelefon, számítógép, laptop) és alkalmazások feltörése, de még inkább az ezekbe történő nem programozói tudást feltételező bejutás.

A bejutás gyakoribb, nem programozói módjai a következők: a „közös barátság és bizalom" elve alapján megadják egymásnak a jelszavakat; a jelszavak jól elérhető és látható helyen vannak; a jelszavak egy beszélgetésben elhangoznak („a kutyám neve kisbetűvel"); a személyt ismerve könnyen kikövetkeztethetőek (pl. kedvenc zenekar/énekes neve, születési idő, háziállat neve).

Megoldási lehetőségek:

– Megértik, hogy van egy olyan része az életnek, amit nem kell megosztaniuk senkivel sem. Mindegy, hogy mi az indok.

– Megpróbálnak megjegyezni egy bonyolultabb, nehezen kikövetkeztethető jelszót.

– Bizonyos időközönként lecserélik a jelszavukat.

5. A fiatalok által használt eszközök vírussal való megfertőzése

Ez sem csak informatikai kérdés, mert pl. egy ismerős(nek tűnő) személytől érkező „I love you" üzenetet és csatolt fájlt tartalmazó levelet az emberek gyakorlatilag életkortól függetlenül megnyitnak. A neten némi kutakodás után lehet találni olyan alkalmazást, ami trójai falóként elküldve képes átvenni az áldozat gépe felett a kontrollt (pl. elküldi a felhasználói neveket és jelszavakat a belépéssel egyidejűleg egy előre beállított e-mail címre). Rendszerint ez is csak gyerekcsínynek tűnhet, mivel ha a támadó nem egy ifjú hacker, akkor az osztálytárs inkább csak kíváncsi, szeretne belesni társa életébe. Mi-

vel azonban nem ismeri a kártevő szoftver valódi működését, így tudtán kívüli károkat is tud vele okozni.

Megoldási lehetőségek:

– Még az ismerős(nek tűnő) személytől érkező e-mailek csatolt állományát sem kell automatikusan megnyitni.

– A telepített szoftverek egy része automatikusan figyelmeztet, ha veszélyt érez. Ezt a figyelmeztetést nem érdemes figyelmen kívül hagyni.

– A fizetős vírusellenőrzők mellett számos szabadon használható, térítésmentes változat is rendelkezésre áll, célszerű ezek közül egyet telepíteni az informatikai eszközre.

6. A fiatalok által használt eszközökről és/vagy távoli tárhelyeikről (felhő) történő adatlopás

Ezt ugyan külön kategóriaként említem, de az esetek egy részében a fenti módon történik a behatolás. Az is viszonylag gyakorinak mondható, hogy az eszközökbe vagy eleve jelszó nélkül lehet belépni, vagy ugyan jelszó használatával, de a belépés után nincs semmilyen időkorlát, vagyis ha a gépet rövidebb-hosszabb időre magára hagyja a felhasználó, a támadó akkor is használni tudja.

Megoldási lehetőségek:

– lásd 5. pont;

– belépési jelszó vagy egyéb egyedi azonosításra alkalmas megoldás használata (pl. ujjlenyomatolvasó);

– olyan alkalmazás használata, amelyiknél lehetőség van az azonosításnál az időkorlát beállítására. Ha nem történik billentyűzetleütés, illetve egérmozgás, akkor rövid időn belül zárolja a gépet, ami csak a jelszó ismételt megadásával oldható fel.

7. A fiatalok által használt eszközökön és/vagy távoli tárhelyeiken (felhő) történő adatmódosítás

Ez hasonlít a 4. pontnál leírtakhoz azzal a lényeges különbséggel, hogy az adatmódosítás nehezebben érhető tetten. Egyszerűbb esetekben bizonyos szöveges/képi anyagokban történik változtatás (pl. kép retusálása, szöveg módosítása), de megeshet, hogy eleve a hozzáférési adatokat módosítja a támadó.

Megoldási lehetőség: lásd 4. pontban leírtakat.

8. A fiatalok által használt eszközökön és/vagy távoli tárhelyeiken (felhő) található adatok törlése

Ez az eset hasonlít részint a 3., részint a 6. és 7. pontban leírt esetekre. Itt a cél nem az adatok újbóli felhasználása, hanem végleges megsemmisítése (pl. kompromittáló képek).

Megoldási lehetőségek:

– lásd 6. pont;

– a valóban fontos adatokról célszerű egy teljesen más helyen/eszközön biztonsági másolatot is tárolni.

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

Ennek kivédése elsősorban a szolgáltatók dolga. A fiatalokat annyiban érheti hátrány, hogy ha pl. az iskolai feladataik elkészítéséhez korábban rendszeresen látogatott hely elérhetetlenné válik, akkor megeshet, hogy nem tudják időben beadni a házidolgozataikat.

10. A fiatalok által látogatott weboldalakon található tartalmak hitelessége

A fiatalok házidolgozataik egyre nagyobb részét készítik el úgy, hogy hivatkozásaik kivétel nélkül a neten is megtalálható tartalmakra vonatkoznak. Sajnos még a Wikipédia esetében is beigazolódott, hogy vannak olyan tartalmak, amelyeket bizonyos érdekcsoportok saját céljaik érdekében elferdítettek.

Megoldási lehetőség: az oktatók hangsúlyosabban hívják fel a diákok figyelmét arra, hogy a netes forrásokat kezeljék kellő kritikai fenntartásokkal, vagy olyan oldalakat látogassanak meg, amelyeket a tanár javasol. Célszerű, ha a tanuló megtekinti a könyvtárban található nyomtatott forrásokat is.

11. A fiatalok által látogatott weboldalakon található tartalmak illetéktelen módosítása

Ennek kivédése rendszerint a szolgáltató és/vagy szerkesztők felelőssége.

12. A fiatalok adatait tartalmazó adatbázisok feltörése, s onnan az adatok ellopása

Ennek kivédése rendszerint a szolgáltató felelőssége.

Megoldási lehetőségek:

– Tudatosítani a fiatalokban, hogy nem szükséges minden, számukra ismeretlen helyen regisztrálniuk.

– Ha mégis kíváncsiak, akkor hozzanak létre csak erre a célra használt e-mail címet, illetve alkossanak meg egy hamis profilt.

– Azt is célszerű tudatosítani a fiatalokban, hogy ha számos olyan helyen regisztrálnak, amelyiknél e-mail címet és jelszót kell megadni, akkor érdemes mindenhol legalább más jelszót használni. Ha ugyanis az e-mail cím és jelszó páros megegyezik mindenhol, akkor egy adatbázis feltörése révén könnyen hozzá lehet férni a felhasználók más adatbázisokban levő fiókjaihoz is.

13. A fiatal az életkorából adódó szellemi és értelmi színvonalára, illetve fejlődésére káros tartalmakat tud elérni.

Ha ezek törvénybe ütköző tartalmak, akkor a szülő kötelessége (is) ezekről jelentést tenni a hatóságnál.

Megoldási lehetőségek:

– Tudatosítani a fiatalokban, hogy ezek a tartalmak még nem nekik valók (sajnos a kíváncsiság rendszerint erősebb bennük, mint a szülői intelem megfogadása).

– A fiatalok által használt eszközökre olyan alkalmazást telepíteni, amelyik blokkolja az életkoruknak nem megfelelő tartalmak megjelenítését.

14. A fiatal a számára (is) veszélyes bűnözői csoportok hálójába kerül

Ennek több lehetősége is lehet:

Pedofilok: rendszerint más személyiségét veszik fel az interneten, pl. híres celeb vagy annak menedzsere/barátja, közel azonos korú fiatal, a szülők barátja/munkatársa, osztálytárs, távoli rokon. A megfontolt pedofilok valószínűleg attól függően választják ki az avatarjukat, hogy milyen módon és mit akarnak a fiataltól. Ha „csak" a netes zaklatás,

az intim képek megszerzése a cél, akkor gyakorlatilag az azonos korú fiatal, a szerelmetes osztálytárs, a híres celeb vagy annak fiatal és vonzó menedzsere a megszemélyesített ismerős. Ha a bűnelkövetés a valódi világban is realizálódhat (pl. nemi erőszak, zsarolás), akkor vélhetőleg a szülők barátja/munkatársa, a távoli rokon egyaránt lehet választott szerep.

Szélsőséges nézeteket valló csoportok (pl. terrorszervezetek): a fiatalok pillanatnyi szomorúságát, reményvesztettségét, hullámzó kedélyállapotát használják ki, a boldogság, a jobb élet, az elismertség és egyéb, a fiatal számára is vonzó lehetőségek felvázolásával. Céljuk, hogy a fiatal a csoport tagja legyen, esetleg olyan helyzetekbe keverik, hogy egy lebukásnál csak a naiv és gyanútlan fiatalt tudja a rendőrség azonosítani, mint bűnelkövetőt.

Kíberbűnözők: célpontjaik olyan fiatalok, akik rendszerint introvertált személyiségek, nagyon jól értenek a számítástechnikához, az informatikához, gyakorlatilag egész nap a gép előtt ülnek, s ahelyett, hogy játszanának/tanulnának/szórakoznának, frissen megszerzett tudásukkal tesztelik a céges/kormányzati oldalak feltörhetőségét. Bevett gyakorlat, hogy egy viszonylag könnyen feltörhető oldalt hoznak létre a bűnözők, melyet a fiatal fel is tör. Ezután „levadásszák", s megfenyegetik, hogy ha nem tesz meg számukra bizonyos dolgokat, feljelentik a rendőrségen, a gyámhivatalnál stb.

Csalók: céljuk, hogy a fiataltól adatokat, bizalmas információkat, esetleg valamilyen nemes ügy (pl. állatvédelem) érdekében pénzt (vagy azzal egyenértékűként bankszámla hozzáférési adatokat) csaljanak ki.

Megoldási lehetőségek:

– Tudatosítani a fiatalban (tanár, szülő, esetleg idősebb, érettebb testvér felelőssége), hogy az őszinteségéért nem kap büntetést, ha hibát követett el, akkor is értékes és szeretik.

– Tudatosítani a fiatalban, hogy célszerű a ballépését minél előbb elmondania egy számára hiteles személynek, hogy a probléma ne súlyosbodjon, s minél hamarabb meg lehessen kezdeni annak elhárítását.

– Megtenni a rendőrségen a bűnözőkkel, bűnbandákkal szemben a büntetőfeljelentést.

– Szorgalmazni a rendőrségen, hogy mihamarabb hivatalosan lépjenek fel nemcsak a bűnözők, hanem a tevékenységük és nézeteik megosztására használt odalak/platformok/fórumok tulajdonosai/üzemeltetői ellen is.

Mivel a Z generáció rendszerint még a szüleivel él együtt, ezért érdemes legalább említés szintjén arról is szólni, hogy a *szülőket is védeni* kell, s biztosítani kell esetükben is az információbiztonságot. Ennek néhány fontosabb lépése:

– A fiatal lehetőleg ne használja a szülők technikai eszközeit (vagy ha igen, akkor szülői felügyelet mellett).

– Ha ez nem oldható meg, akkor legalább jelszóval védjék a közösen használt gépen található könyvtárakat, s állítsák/állíttassák be, hogy a fiatal nem lehet teljes értékű felhasználója a gépnek rendszergazdai jogokkal.

– A családi nyomtató/scanner egy olyan gépen legyen, amelyik nem tartalmaz bizalmas és fontos adatokat, s így bármelyik családtag hozzáférhet.

– Ha van családi szerver, illetve hálózati adattároló (NAS) vagy médiaszerver, akkor ott a szülők rejtsék el gyermekeik elől a bizalmas és fontos adatokat tartalmazó könyvtárakat.

– Ahogy a fiataloknak, úgy szüleiknek is illik fejben tartani a jelszavaikat.

Összefoglalás

Tanulmányomban az európai Z generációt érintő két hangsúlyos aspektussal foglalkoztam: az oktatással és az információbiztonsággal. A statisztikai adatok elemzésekor láthattuk, hogy ez a generáció az Európai Unió 28 tagállama összlakosságának közel egyhetedét teszi ki. Rámutattam arra, hogy a Z generációsok s az őket követő valamennyi generáció már beleszületett az internetbe, a digitális kor világába, így már koragyermekkori szocializációjukban a digitális platformok (eszközök, programok, alkalmazások), illetve a platformokon található tartalmak jelentős szerepet játszanak. Láthattuk, hogy a generáció igazi tanítói (információközlői) részint saját nemzedékének a tagjai, részint a rendszerint idősebb generációk által tulajdonolt infokommunikációs platformok. A Z generáció – életkorából adódóan, s így komolyabb élettapasztalat hiányában – ki van téve az interneten (is) működő bűnözői csoportok támadásainak, ezért az információbiztonság humán aspektusa – beleértve a támadások kivédésére irányuló felkészítésüket, oktatásukat, információ- és adatvédelmi tudatosságukat – kiemelt jelentőséggel és fontossággal bír számukra.

Irodalom

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

Gyaraki Réka Eszter (2015): Számítógépes bűncselekmények és az ellenük való védekezés. In.: Christián László (szerk.): *Információvédelem.* NKE Szolgáltató Kft., Budapest, 175–222.

Haig Zsolt (2015): *Információ Biztonság Társadalom.* NKE Szolgáltató Kft., Budapest.

Horváth Dóra és Mitev Ariel (2015): *Alternatív kvalitatív kutatási kézikönyv.* Alinea Kiadó, Budapest.

Kehal, H. S. és Singh, V. P. (2004): *Digital Economy: Impact, Influences and Challenges.* Idea Group Publishing, London.

Ketskeméty László, Izsó Lajos és Könyves Tóth Előd (2011): *Bevezetés az IBM SPSS Statistics programrendszerbe.* Artéria Stúdió Kft., Budapest.

Kollár Csaba (2011a): *A budapesti ifjúság fogyasztói csoportkultúrája az infokommunikációs társadalomban, és ennek marketingkommunikációs aspektusai.* PREMA Consulting, Budapest.

Kollár Csaba (2011b): Digitális nemzedékek Magyarországon és külföldön. In: Borgulya Ágnes és Deák Csaba (szerk.): *Vállalati kommunikáció a 21. század elején.* Z-Press Kiadó, Miskolc, 217–232.

Kollár Csaba (2012): A kiterjesztett valóság (AugmentedReality) (nem csak) üzleti és marketinges lehetőségei. In: Farkas Atila, Kollár Csaba és Laurinyecz Ágnes (szerk.): *A filozófia párbeszéde a tudományokkal: A 70 éves Tóth Tamás professzor köszöntése.* Protokollár Tanácsadó Iroda, Budapest, 159-171.

Kollár Csaba (2014a): Életünk a digitális korban. In.: Kollár Csaba és Tóth Renáta (szerk.): *Pedagógia a digitális korban.* PREMA Consulting, Budapest, 1-30.

Kollár Csaba (2014b): *Kísérleti jegyzet a digitális kommunikáció című tantárgyhoz 2.0 változat.* PREMA Consulting, Budapest.

Lessig, L. (2004): *Free culture. How Big Media UsesTechnology and the Law toLock Down Culture and ControlCreativity.* Penguin Group, New York.

Levine, R., Locke, C., Searls, D., Weinberger, D. (2001): *The Cluetrain Manifesto: The End of Business as Usual.* Basic Books, New York.

Mitnick, K. D. és Simon, W. L. (2006): *A legendás hacker. A behatolás művészete.* Perfact-Pro Kft., Budapest.

Nábrády Mária (2014): *A megtévesztés művészete.* Libri Kiadó, Budapest.

Saphiro, C. és Varian, H. R. (1999): *Information Rules: A Strategic Guidetothe Network Economy.* Harward Business School Press, Boston.

Schneier, B. (2010): *Schneier a biztonságról.* HVG Kiadó, Budapest.

Wallace, P. (2002): *Az internet pszichológiája.* Osiris Kiadó, Budapest.

Warren, P. és Streeter, M. (2005): *Az internet sötét oldala.* HVG Kiadó, Budapest.

Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, Az Európai Unió Alapjogi Chartája http://europa.eu/eu-law/decision-making/treaties/pdf/consolidated_versions_of_the_treaty_on_european_union_2012/consolidated_versions_of_the_treaty_on_european_union_2012_hu.pdf (letöltés ideje: 2016. 03. 14.)

Eurostat statisztikái - http://ec.europa.eu/eurostat/web/population-demography-migration-projections/population-data/database (letöltés ideje: 2016. 03. 14.)

Jegyzetek

1 Az Európai Unió tagállamainak szakértői által készített tanulmányok, illetve a nemzetközi szakirodalom sem képvisel egységes álláspontot az egyes generációk születési idejére s életkori intervallumára vonatkozóan. Jelen tanulmányban ezek az intervallumok a szerző korábbi kutatásai és tanulmányai alapján kerültek meghatározásra. Az egyes generációk elemzése ugyan életkori intervallumok szerint történik, de nem a születési évek egységes meghatározása a fontos, hanem az, hogy az egyes generációk között milyen különbségek, illetve hasonlóságok figyelhetőek meg.