

PRO PUBLICO BONO MAGYAR KÖZIGAZGATÁS



2015 4

A NEMZETI KÖZSZOLGÁLATI EGYETEM ÁLLAM-
ÉS KÖZIGAZGATÁS-TUDOMÁNYI SZAKMAI FOLYÓIRATA



PRO PUBLICO BONO – Magyar Közigazgatás

A NEMZETI KÖZSZOLGÁLATI EGYETEM ÁLLAM- ÉS KÖZIGAZGATÁS-TUDOMÁNYI SZAKMAI FOLYÓIRATA

szerkesztőbizottság

A SZERKESZTŐBIZOTTSÁG ELNÖKE:

Prof. Dr. Kiss György dékán, egyetemi tanár (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar)

FŐSZERKESZTŐ:

Dr. Fejes Zsuzsanna tanszékvezető, egyetemi docens (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar)

A SZERKESZTŐBIZOTTSÁG TISZTELETBELI ELNÖKE:

Prof. Em. Dr. Tamás András (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar)

SZERKESZTŐBIZOTTSÁGI TAGOK:

Dr. Biró Marcell közigazgatási államtitkár (Miniszterelnöki Kabinetiroda) • *Dr. Bitskey Botond* főtitkár (Alkotmánybíróság) • *Dr. Cserny Ákos* egyetemi docens (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar, Közjogi Intézet) • *Prof. Dr. Kukorelli István* egyetemi tanár (Eötvös Loránd Tudományegyetem, Állam- és Jogtudományi Kar) • *Dr. Hazafi Zoltán* intézetvezető, egyetemi docens (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar, Életpálya és Emberi Erőforrás Intézet) • *Dr. Horváth Attila* intézetvezető, egyetemi docens (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar, Állam- és Társadalomelméleti Intézet) • *Dr. Imre Miklós* intézetvezető, főiskolai tanár (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar, Közjogi Intézet) • *Dr. Janza Frigyes* főtitkár (Rendészettudományi Társaság) • *Dr. Kis Norbert* továbbképzési és nemzetközi rektorhelyettes, főiskolai tanár (Nemzeti Közzolgálati Egyetem) • *Prof. Em. Dr. Máthé Gábor* (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar, Állam- és Társadalomelméleti Intézet) • *Dr. habil. Müller György* egyetemi magántanár (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar, Állam- és Társadalomelméleti Intézet) • *Prof. Dr. Nemeslaki András* intézetvezető, egyetemi tanár (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar, E-közzolgálati Fejlesztési Intézet) • *Prof. Dr. Papp Tekla* tanszékvezető, egyetemi tanár (Nemzeti Közzolgálati Egyetem, Nemzetközi és Európai Tanulmányok Kar, Európai Köz- és Magánjogi Tanszék) • *Prof. Dr. Patyi András* rektor, egyetemi tanár (Nemzeti Közzolgálati Egyetem) • *Prof. Dr. Torma András* rektor, egyetemi tanár (Miskolci Egyetem) • *Prof. Dr. Török Gábor* intézetvezető, egyetemi tanár (Nemzeti Közzolgálati Egyetem, Közigazgatás-tudományi Kar, Civilisztikai és Nemzetgazdasági Intézet) • *Prof. Dr. Varga Zs. András* dékán, egyetemi tanár (Pázmány Péter Katolikus Egyetem, Jog- és Államtudományi Kar)

KÜLFÖLDI TISZTELETBELI TAGOK:

Jan Bárta Cseh Tudományos Akadémia (Prága) • *Daniel Klimovsky* Szlovák Műszaki Egyetem (Kassa) • *Zdenek Koudelka* Masaryk Egyetem (Brno) • *Herbert Küpper* Institut für Ostrecht (Regensburg) • *Walter Maier* Ludwigsburgi Közigazgatás-tudományi és Pénzügyi Főiskola (Ludwigsburg) • *Daniel Szergej Naumov* P. A. Sztolipin Volga-menti Közzolgálati Akadémia (Szaratov) • *Tóth Mihály* Ukrán Nemzeti Tudományos Akadémia (Kijev) • *Igor Palús* Pavol Jozef Safárik Egyetem (Kassa) • *Ewa Poplawska* Lengyel Tudományos Akadémia (Varsó) • *Jan Ziekow* Német Közigazgatási Kutatóintézet (Speyer) • *Prof. Dr. Li Junqing* Minzui Egyetem (Peking)

PRO PUBLICO BONO – Magyar Közigazgatás

4. SZÁM

köszöntő	NEMESLAKI ANDRÁS	2
tudományos közlemények/ tanulmányok	KŐ ANDREA – SZABÓ ZOLTÁN	
	• Innovatív e-egészségügyi megoldások – A jövő internetes technológiai a távmonitorozásban	6
	RÉPÁS SÁNDOR – DALICSEK ISTVÁN	
	• Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében	22
	MICHELBERGER PÁL – DOMBORA SÁNDOR	
	• A felhasználói profil szerepe az információbiztonságban	34
	ORBÁN ANNA	
	• Ügyfél-elégedettség mint a hatékonyság egyik dimenziója	51
	BENCSIK ANDRÁS – FÁBIÁN ADRIÁN – PÁL EMESE – SZŐKE GERGELY LÁSZLÓ	
	• A közigazgatás és a média kapcsolódási pontjai	60
	NEMESLAKI ANDRÁS – SASVÁRI PÉTER	
	• A felhőalapú számítástechnika használata a köz- és üzleti szférában	76
szakmai fórum	NAGYNÉ TAKÁCS VERONIKA – KOVÁCS LÁSZLÓ	
	• Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai	85
	ORBÁN ZSOLT – BALKÁNYI PÉTER	
	• E-learning-tananyagok fejlesztése a közigazgatásban	100
	TÖRLEY GÁBOR – SASVÁRI PÉTER	
	• A magyar közigazgatást kutatók tudományos láthatósága	112
nemzetközi kitekintés	JUHÁSZ LILLA MÁRIA – PAKSI-PETRO CSILLA – PEDRO REIS	
	• Virtual learning all over the World. Good practice from Portugal	133
szemle	KISS ATTILA – BELÁZ ANNAMÁRIA	
	• Szabályozás és egységesítési törekvések az IKT és a távközlés világában. Beszámoló az ITU 2015 konferencia eredményeiről és annak háttéréről	146
tájékoztató	Szerzőinkhez	158
	Idegen nyelvű tartalomjegyzék	160
	Impresszum	163

2015

Köszöntő

A szerkesztőbizottsági megbeszéléseink alapján nagy örömmel és megtiszteltetéssel vállaltam, hogy 2015 utolsó számának vendégszerkesztője legyek. Olyan számmal szeretnénk búcsúztatni ezt az évet, egyúttal pedig megkezdeni a 2016-osat, amelyik a közigazgatás- és államtudomány egyik legdinamikusabban fejlődő, ezáltal talán a legtöbb vitát kiváltó területével foglalkozik; nevezetesen azzal, hogy az infokommunikációs technológiák (IKT) hogyan hatnak a közszolgálat és az állam működésére. Izgalmas időszakban vállalkoztunk kollégáimmal és a szám szerzőivel erre, egyrészt a magyar közszolgálat fejlesztése, másrészt az államtudomány körül fellángoló viták szempontjából.

A 2014–2020-as időszakban a Közigazgatási és Közszolgáltatás-fejlesztési Operatív Program (KÖFOP) keretében több mint 240 milliárd Ft értékű fejlesztésre nyílik lehetőség a magyar állam működésének modernizálására. Ha ehhez azokat a forrásokat is beszámítjuk, amelyek nem címkézetten a közigazgatást célozzák, pl. a Gazdaságfejlesztési és Innovációs Operatív Programot (GINOP), a Versenyképes Közép-Magyarország Operatív Programot (VEKOP), vagy akár más operatív programokat, akkor könnyen beláthatjuk, hogy a következő öt évben olyan lehetőségek állnak a magyar állam fejlesztése előtt, amelyek 2020 után források vonatkozásában nem lesznek. Ezen programok szinte mindegyikének kulcselme az IKT; az alkalmazások elterjesztése, a hatékonyság és versenyképesség növelése, az állampolgárokat és vállalatokat érintő adminisztratív terhek csökkentése, illetve azoknak a képességeknek és ismereteknek a fejlesztése, amelyek az IKT-befogadást – a digitális szakadékok csökkentését – lehetővé teszik. Az operatív programok figyelembe veszik azt is, hogy a közszolgáltatások és közigazgatási folyamatok ilyen ambiciózus fejlesztése csak olyan hálózati infrastruktúrán képzelhető el, amely minden állampolgár számára elérhető, magas minőségben, megbízhatóan és biztonságosan működik úgy, hogy megvédi az egyénetet és az államot a kibertérből érkező fenyegetésektől.

A források felhasználásával kapcsolatban az előttünk álló időszakban számos kutatásra nyílik lehetőség, mind elméleti, mind empirikus szemléletben. Pragmatikus és új eredményekre van szükségünk többek között a közigazgatási IKT-rendszerek fejlesztésével kapcsolatban, a technológia befogadásának mélyebb megértésére, a közszolgálati szervezetek innovációjának javítására, a közszolgálati tudásmenedzsment elmélyítésére. Szükség lesz a közigazgatási folyamatok átszervezésére, az IKT innovációs gerjesztő hatásának kiterjesztésére, az egyes szakigazgatási rendszerek működésének átalakítására, sőt, a szakpolitikai gondolkodás szociotechnikai irányú elmélyítésére is; az állam kibertérben való működésének – ha úgy tetszik a digitális állam koncepciójának – részletes kidolgozására. A környezeti kihívásoknak való megfeleléshez új ismeretekre van szükségünk az információ- és adatvédelem területén, a biztonságos IKT-infrastruktúra működtetésével kapcsolatosan, és nem utolsósorban a hatékony program- és projektmenedzsment-módszertanok elterjesztésére, amelyek kimondottan a közszolgálat és közigazgatás sajátosságainak felel-

nek meg. Az operatív programok befektetésének sikere, a következő öt év beruházásainak megtérülése nagymértékben függ ezektől az interdiszciplináris kutatásoktól.

Az IKT államra, annak működésére gyakorolt hatásának vizsgálata tudományelméleti szempontból is jelentős. Az internet radikális átformáló hatása (disruptive innovation) az 1990-es évek közepétől egyre több iparágon söpört végig, teljes mértékben átalakítva azok szerkezetét és működési modelljét. A médiaipar, a járműipar, a közlekedés, a kiskereskedelem, a turizmus, az oktatás, az egészségügy felismerhetetlenségig átalakult az elmúlt 25 évben; az IKT megváltoztatta az értéktermelés folyamatait, a szereplők érdekviszonyait, a termékek és szolgáltatások jellegét, és a foglalkoztatáshoz szükséges képességeket és ismereteket. Az információs gazdaság működésének, illetve a jólét növelésének egyre szembetűnőbb szűk keresztmetszete a hiányosság az állam működésének az információs kornak megfelelő átgondolásában. A technológia, illetve a technogazdasági paradigmák vizsgálata a közgazdaságtudomány perifériáján húzódik, ezzel számos jelenség és narratíva megértése nehéz az állam változó szerepével, a társadalomhoz és gazdasághoz való viszonyával kapcsolatban. A tudomány-technika elméletek köre (Science Technology Studies) egyike azoknak a transzdiszciplináris irányoknak, amelyek az államtudományt meg tudják erősíteni, relevánsá tudják tenni a modern kihívásokkal szemben, sőt más tudományokkal szemben való hozzáadott értékét is ki tudják alakítani (pl. a jogtudományhoz, politikatudományhoz vagy gazdaságtudományhoz viszonyítva).

Az IKT ugyanakkor általános értelemben is hatást gyakorolt a tudományra mint „iparágra”, az állam- és közgazdaságtudományon túlmutatva is. Az internet nemcsak a személyes és üzleti kommunikációt alakította át, hanem megváltoztatta a tudományos kutatás és publikálás módját is, a tudományos teljesítmény mérését, és konkrétan azt is, hogyan válik láthatóvá és ismertté egy tudományterület, illetve annak kutatói. Különösen érdekes ebből a szempontból Sasvári Péter és Törley Gábor kollégáim cikke a szakmai fórum rovatban, amelyik tudományometriai szempontból dolgozza fel a Pro Publico Bono szerzőinek munkásságát. Pontosan azt az új tudományos kihívást elemzik, miként használható az IKT a tudományos teljesítmény növelésére. Eredményeik alapján megoldásokat javasolnak a tudományos repozitóriumok, a közösségi média és a nyílt forráskódú rendszerek használatára azért, hogy az államtudomány teljesítménye láthatóbb, és kutatási eredményei elérhetőbbek legyenek.

Amennyiben az olvasó valamilyen rendszerben szeretné átolvasni a szám cikkeit és ez alapján szeretne képet kapni a fenti problémákról, akkor a tanulmányok olvasását az alábbi sorrendben javaslom:

Kiss Attila és Béláz Annamária az IKT-szektor gazdasági jelentőségét mutatja meg a 2015 őszi Magyarországon rendezett ITU Világkonferencia beszámolójának keretében. Az IKT-szektor és az állam viszonya, együttműködésük jellege nemcsak a közgazdaságtudomány fejlődésének szempontjából kiemelkedő, hanem azért is, mert ez a viszony az egész nemzetgazdaság

növekedési és innovatív képességét, a foglalkoztatás szerkezetét, és nem utolsósorban a jóléti állam számos feladatának hosszú távú sikerét (egészségügy, oktatás, nyugdíjrendszer, szociálpolitika) meghatározza.

Öt cikk mutat be friss kutatási eredményeket egy-egy szakpolitikai területen, amelyek informatikai fejlesztésekhez kapcsolódnak.

A tanulmányok rovatban Kő Andrea és Szabó Zoltán innovatív megoldásokat mutatnak be az egészségügy területén, elsősorban a távmonitorozásban. Bencsik András, Fábian Adrián, Pál Emese és Szőke Gergely László a közigazgatási jog és a modern média kapcsolódási pontjait elemzik két fontos szempontból; az átláthatóság és a jogi felügyelet nézőpontjából. Orbán Anna az IKT-alkalmazás egyik legfontosabb közigazgatási elvárását elemzi, nevezetesen a hatékonyság javításának lehetőségeit, kiemelten annak mérését. Bemutatja a Jó Állam Jelentés hatékonyságdimenzióját (hozzáférhetőség, ügyfélteher, erőforrás-gazdálkodás, felkészültség, elégedettség), és kiemelten vizsgálja ezeken belül az állampolgárok viszonyát a közigazgatással: hogyan mérhetjük és javíthatjuk az állam működését ezen a területen. Az oktatás átalakításának eredményeit mutatja be a szakmai fórumon Orbán Zsolt és Balkányi Péter, kiemelten a tananyagfejlesztés és disszemináció modernizálását, az e-learningben rejlő lehetőségeket a közigazgatási továbbképzésben; illetve Juhász Lilla Mária, Paksi-Petró Csilla és Pedro Reis az e-learning közigazgatási képzésben való használatát hasonlítják össze Portugália és a magyar közigazgatás keretrendszerével.

Az IKT elmúlt években zajló fejlődése lehetővé tette, hogy a felhasználó szervezetek szolgáltatásként használják és vegyék igénybe annak funkcióit. Ehhez szükség volt a szélessávú internet elterjedésére, az IKT-szolgáltatások kialakulására, és nem utolsósorban az IKT beépülésére a szervezetek munkafolyamataiba. Ennek a szolgáltatási szemléletnek az alapjait, és közszolgálatban rejlő lehetőségeit, valamint kihívásait mutatjuk be Sasvári Péter kollégámmal az informatikai felhő görcsö alá vételével a tanulmányok rovatban.

Végül három cikk azt a kérdést járja körbe, hogy melyek a kihívások abban a tekintetben, hogy az internet nemcsak szolgáltatásaink és munkavégzésünk új „tere”, nemcsak személyes szféránk kiterjesztése, hanem a 21. századra az egyik legkockázatosabb kritikus infrastruktúránk lett. Sajnos a hálózatokon keresztül támadhatóak lettünk, a személyes és közadatok újszerű veszélybe kerültek, az információszabadság és átláthatóság fontos értéke fenyegetettségbe került, a terrorizmus nemcsak fizikai létünk védelmét, hanem az ún. kibertér biztonságának megvédését is kiemelt feladattá teszi az állam számára.

Az információbiztonsághoz kapcsolódóan a szakmai fórumon Nagyné Takács Veronika és Kovács László annak az egyedülálló elektronikus információbiztonsági vezető szakirányú továbbképzésnek az első tapasztalatait összegzik, amelyet a Nemzeti Kibervédelmi Stratégia keretében született információbiztonsági törvény előírásának (lásd Ibtv.) megfelelően a Nemzeti Közszoigálati Egyetem végez. Ezek a szakemberek ugyanis kiemelt szere-

pet fognak játszani a közeljövőben azoknak az elveknek a megismertetésében és bevezetésében, amelyek a közszolgálati szervezetek kibervédelmének javítását, a biztonságtudatos-
ságot és a támadások kezelését segítik. Az információbiztonság elméleti kérdéseivel foglalkozik két kutatás a tanulmányok rovatunkban; Répás Sándor és Dalicsek István a kockázatok kezelésének módszertanát mutatja be, míg Michelberger Pál és Dombora Sándor a felhasználói profilok készítésének jelentőségét ismertetik, azt, hogy milyen gyenge láncszem az egyéni felhasználó, az ő sokszor akaratlan hibái, aminek elemzésével csökkenthetjük a kialakuló veszélyhelyzeteket.

A szám szerkesztésekor nem törekedtünk teljességre vagy valamilyen átfogó koncepció bemutatására, azt gondolom, ez pontosan a jövő kihívása; a bemutatott problémakörökkel kapcsolatban a Budapesti Corvinus Egyetem, a Miskolci Egyetem, a Nemzeti Közszolgálati Egyetem, az Óbudai Egyetem és a Pécsi Tudományegyetem kutatóinak munkái olvashatók. Különösen fontosnak tartom ezt a sokszínűséget, ami nagyon jól érzékelteti az „e-közszolgálat” területkonstruktivista épülését, és az ezzel foglalkozó „láthatatlan kollégium” kiterjedtségét.

Dr. Nemeslaki András
intézetvezető, egyetemi tanár,
E-közszolgálat Fejlesztési Intézet, NKE

• tanulmányok

Kő Andrea – Szabó Zoltán

INNOVATÍV E-EGÉSZSÉGÜGYI MEGOLDÁSOK – A JÖVŐ INTERNETES TECHNOLÓGIÁI A TÁVMONITORINGOZÁSBAN

Az egészségügyi szektor, különösen a közép- és kelet-európai országokban számos kihívással küzd; a képzett munkaerő elvándorol, a társadalom gyorsan öregszik, a finanszírozás nehézkes. Emiatt központi szerephez jut a prevenció és a páciensek egészségügyi állapotának monitorozása. Az e-egészségügy kiemelt fejlesztési területe a 2015-ös Egészségügyi Ágazati Stratégiának¹ is. Ezeket a feladatokat a jövő internetes technológiái (Future Internet Solutions) nagymértékben támogathatják, jelentősen kitágítva a hagyományos kezelés határait. Olyan új, innovatív megoldások jelennek meg az egészségügyben, mint a betegek távmonitorozása az infokommunikációs eszközök által kínált költséghatékony infrastruktúra igénybevételével. Ez a cikk az e-egészségügyi megoldások kihívásait, környezetét elemzi jogi, biztonsági, gazdasági, társadalmi szempontból, valamint röviden bemutatunk egy a jövő internetes technológiájára építő tudásalapú, távmonitorozó megoldást is.

KULCSSZAVAK:

eHealth, mHealth, egészségügyi távmonitorozó megoldások, a jövő internetes technológiái



1. BEVEZETÉS

A GDP-arányos egészségügyi kiadások jelentősen emelkedtek az EU országokban az 1970-es 4,7%-hoz képest 2014-re 9%-ra.² Ráadásul az európai népesség jelentős öregedését jelez-

1 Emberi Erőforrások Minisztériuma: *Egészséges Magyarország 2014–2020; Egészségügyi Ágazati Stratégia*, 2015. Forrás: www.kormany.hu/download/5/60/40000/Eg%C3%A9szs%C3%A9ges_Magyarorsz%C3%A1g_-_e%C3%BC_strat%C3%A9gia.pdf (2015. 12. 21.)

2 Forrás: OECD Health Data 2014; Eurostat Statistics Database; WHO Global Health Expenditure Database.

te előre az ENSZ, pedig Európa már ma is a legöregebb kontinens. A 65 év felettek aránya a munkaképes korú lakossághoz viszonyítva 49%-ra becsülhető,³ 2060-ra minden inaktív személyt 2 aktív munkavállalónak kell eltartania az EU országokban.⁴

Az egészségügyi ellátások számos területe kiemelt figyelmet élvez, így pl. a szív- és érrendszeri betegségek, mint a globálisan legnagyobb számú (jelenleg évi 17,3 millió) haláleset okozói. Ez a szám 2030-ra akár 23,6 millióra is emelkedhet.⁵ Európában az idősek kórházi kezelését elsősorban a krónikus szívproblémák teszik szükségessé (az összes kórházi kezelés 1–2%-a), és egy szívroham miatti kezelés átlagos költsége 10 000 Euro.⁶

A magyar egészségügyi szektor is hasonló, néhány esetben komolyabb problémákkal küzd. A legnagyobb kihívást a közelmúltban az orvosok és a szak személyzet elvándorlása, a finanszírozási gondok, illetve a szív- és érrendszeri betegségek magas előfordulási aránya,⁷ valamint a népesség gyors ütemű előrepedése jelenti.

A közép-kelet-európai régió országokban komoly gond a magasán képzett egészségügyi munkaerő megtartása. Ahogy Béltéczi János, a Magyar Orvosok Szövetségének elnöke a Guardiannek adott interjújában kifejtette: „6 éve minden nap három orvos és két nővér hagyja el az országot”⁸

Az idősebb munkavállalók aránya (55 és 64 év között) a munkaképes korú lakosságban akár 50%-kal is emelkedhet, miközben az EU országokban ez a növekedés csak 18,3% (a 2013-as 12,7% 2060-ra éri el a 21,1%-ot).

Magyarország a szívbetegségekből eredő halálesetek előfordulásának számát tekintve az 5. helyen áll a világon.⁹ Az elhalálozások mintegy 49,4%-a volt visszavezethető szívbetegségekre 2013-ban.¹⁰

A fenti indokok miatt az e-egészségügyi (eHealth) megoldások fontossága egyre nő a világban és Magyarországon is. Számos előnyük között említhető, hogy biztonságos módon egyszerűsítik az adminisztratív eljárásokat, javítják az egészségügyi szolgáltatások elérhetőségét,

3 European Commission: *The 2015 Ageing Report*, 2015. (ISSN 0379-0991)

4 Fabienne ABADIE et al.: *Strategic Intelligence Monitor on Personal Health Systems (SIMPHS) Market Structure and Innovation Dynamics*, European Commission Joint Research Centre, Institute for Prospective Technological Studies, 2011. (ISBN 978-92-79-18947-0)

5 Alan S. Go et al. on behalf of the American Heart Association Statistics Committee and Stroke Statistics Subcommittee. *Heart disease and stroke statistics — 2013 update: a report from the American Heart Association*, *Circulation*, 2013/127 (1).

6 Andreas BUNDKIRCHEN, Robert HG SCHWINGER: *Epidemiology and economic burden of chronic heart failure*, *European Heart Journal Supplements*, 2004/6. (Suppl D: D57–D60).

7 Maier RACHAEL: *Heart Disease Statistics*, 2014. Forrás: www.healthline.com/health/heart-disease/statistics#1 (2014. 12. 22.)

8 Daniel NOLAN: *NHS hiring drive hurts Hungary but India can cope with doctor exodus* = *The Guardian*, 2015. Forrás: www.theguardian.com/society/2015/jan/28/-sp-hungary-india-doctors-nhs-recruitment-drive-effect (2015. 12. 21.)

9 eds. Susan Krauss WHITBOURNE, Martin SLIWINSKI: *The Wiley-Blackwell handbook of adulthood and aging*. Vol. 40., John Wiley & Sons, 2011.

10 Forrás: Hungarian Statistical Office. www.ksh.hu/docs/hun/xstadat/xstadat_hosszu/h_wdsd001a.html (2015. 03. 22.)

megbízhatóságát, minőségét. Több tanulmány^{11,12} szerint az egészségi életút adatokhoz való hozzáférés révén az állampolgárok jelentős költséget és időt spórolhatnak meg, és az egészségügyi szolgáltatók számára is gyorsabbá és eredményesebbé tehetik a szolgáltatási folyamatot.¹³

Az egészségügyben növekvő igény van a megelőzés és a monitorozás gazdaságos megvalósítására, emiatt új megoldások szükségesek, pl. egészségügyi távmonitorozó megoldások, mobileszközökre és okostelefonra épülő alkalmazások. Ezekkel alacsony infrastruktúra-költségek mellett lehet hatékony szolgáltatásokat biztosítani. A mobileszközök, okostelefonok száma növekedést mutat, 2016-ra már 2 milliárd ilyen eszköz lesz majd.¹⁴ Ezek a platformok új, egyedi lehetőségeket kínálnak az egészségügyi szolgáltatások és alkalmazások számára, egyúttal azonban a biztonsággal, a szabályozási és gazdasági környezettel kapcsolatos kérdéseket is felvetnek.

Ebben a cikkben egy az életfunkciókat monitorozó mobilalapú e-egészségügyi alkalmazást (PISCES-megoldás¹⁵) mutatunk be, és a betegek állapotának, fizikai kondíciójának távmonitorozását biztosító rendszerek kapcsán felmerülő kérdéseket tekintjük át. A PISCES-megoldás célja nemcsak a résztvevők egészségi állapotának monitorozása volt, hanem a szükség szerinti reakciók biztosítása és a fizikai teljesítőképesség fejlesztése is. Az alkalmazás kapcsán tárgyaljuk a hasonló célú megoldásokkal kapcsolatos biztonsági, személyiségi jogi, szabályozási, gazdasági és társadalmi kérdéseket is. A PISCES magyarországi tesztje 2014-ben zajlott.

A cikk az alábbi részekből áll:

Elsőként az egészségügyi szektor néhány meghatározó problémájával foglalkozunk, majd áttekintjük a telemonitoring elméleti vonatkozásait. Ezt követően az mHealth megoldások biztonsági, személyiségi jogi, szabályozási, gazdasági és társadalmi vonatkozásait mutatjuk be, és áttekintjük a PISCES pilot működését és tapasztalatait. Végül értékeljük a PISCES-megoldás erősségeit és gyengeségeit, valamint továbbfejlesztési lehetőségeit.¹⁶

11 Catherine KLERSY et al.: *Economic impact of remote patient monitoring: an integrated economic model derived from a meta-analysis of randomized controlled trials in heart failure*, European Journal of Heart Failure, 13(2011)/4, 450–459.

12 Jolene HUNTER, Richard E. SCOTT: *Considering the Socio-Cultural Impact of E-Health = Global Telehealth: Selected Papers from Global Telehealth 2010 (GT 2010): 15th International Conference of the International Society for Telemedicine and EHealth and 1st National Conference of the Australasian Telehealth Society*, IOS Press, 2010, Vol. 161., 77.

13 Karl A. STROETMANN et al.: *eHealth is Worth it. The economic benefits of implemented eHealth solutions at ten European sites*, Published by the European Commission. Forrás: http://ec.europa.eu/information_society/activities/health/docs/publications/eHealthimpactsept2006.pdf (2010. 10. 25.)

14 *2 Billion Consumers Worldwide to Get Smart(phones) by 2016*. Forrás: www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694 (2014. 08. 25.)

15 A PISCES távmonitorozó megoldást az EUREKA_HU_12-1-2012-0007 – PISCES – Future Internet megoldások támogatása az egészségügyben (CPP2011/1-3 – PISCES – Promoting Future Internet Solutions in Health Environments) projektben fejlesztettük ki

16 PISCES – Promoting Future Internet Solutions in Health Environment (Celtic Plus CPP2011/1-3), The project is supported by the Hungarian Research and Technology Innovation Fund, (New Széchenyi Plan EUREKA_20_12-1-2012-0007)

2. AZ E-HEALTH-TŐL AZ M-HEALTH FELÉ – SZAKIRODALMI ÁTTEKINTÉS

2.1. Az *mHealth* fogalma, története

Az eHealth koncepció viszonylag hosszú történettel bír, az IT-támogatás alkalmazása az egészségügyi ellátásban számos országban bevett gyakorlat. Az első eHealth alkalmazások az egészségügyi adminisztrációra koncentráltak (egészségügyi, ellátási adatok feldolgozását és tárolását oldották meg velük), később klinikai döntéstámogató rendszerek, telemedicina megoldások is elterjedtek. Manapság az elektronikus betegrekord (országos átfogó nyilván-tartás) alkalmazásával lehet biztosítani az egészségügyi szolgáltatást nyújtó szervezetek közt a betegadatok megosztását. Az IT mára az egészségügyi szolgáltatások szerves része, amely hatékonyabb folyamatokat, jobb minőségű szolgáltatásokat, hatékonyságjavulást és a szolgáltatások szélesebb körű elérhetőségét biztosítja.¹⁷

A technológiai evolúció eredményeként, különösen a mobiltechnológiák fejlődésével elindult az eHealth megoldások kiterjesztése *mHealth* alkalmazásokká. A kommunikációs technológiák széles körű használata új lehetőségeket nyitott az eHealth szolgáltatások és a mobilkommunikáció integrációjával. Az *mHealth* úgy definiálható, mint „vezeték nélküli hálózaton és kommunikáción alapuló mobil informatikai alkalmazás, amely egészségügyi szolgáltatásokat, funkciókat nyújt és terjeszt ki, miközben a felhasználó (beteg) számára mozgásszabadságot biztosít”.^{18, 19}

Az *mHealth* szolgáltatások egyik meghatározó területe a távmonitorozás, ami mobil eszközök segítségével biztosítja a beteg életjeleinek, biológiai jelzéseinek mérését a kórházi környezeten kívül. A monitorozó, adatgyűjtő és elemző megoldások széles körű alkalmazása az egészségügyi szolgáltatások standard részévé válhat, miközben egyre jobb, felhasználóbarát és eredményes alkalmazások készülnek. A specifikus igényeknek megfelelően a monitorozás és adatgyűjtés történhet periodikus és folyamatos mérési módszerrel is. Különböző életjelenségek mérhetők, pl. ElectroEncephaloGram (EEG), MagnetoEncephaloGram (MEG), Galvanic Skin Response (GSR), ElectroCardioGram (ECG). Egyéb paraméterek is megfigyelhetők, pl. szívritmus (Heart Rate Variability, HRV). Ez a megközelítés nemcsak az adatok pontosságát javítja az adminisztrációs hibák kiszűrésével, hanem az egészségi adatok szélesebb körű elérhetőségét is biztosítja.²⁰

Amíg a betegek távmonitorozása gyakran csak otthoni környezetben használható, rögzített kommunikációs hálózati csatornán keresztül történik, addig a mobil megoldások nagyobb mozgásszabadságot adnak, így alkalmasak a mindennapi élethelyzetekben (séta, kö-

17 ed. Joseph TAN: *E-health care information systems: an introduction for students and professionals*, John Wiley & Sons, 2005.

18 Pavin PAWAR et al.: *A framework for the comparison of mobile patient monitoring systems*, Journal of biomedical informatics, 45(2012)/3, 544–556.

19 Kyle Leon WEST: *mHealth: A Comprehensive and Contemporary Look at Emerging Technologies in Mobile Health*. Forrás: trace.tennessee.edu/cgi/viewcontent.cgi?article=2711&context=utk_chanhonoproj (2014. 08. 26.)

20 WHO: *mHealth: New horizons for health through mobile technologies: second global survey on eHealth*, 2011. (ISBN 978-92-4-156425-0). Forrás: www.who.int/goe/publications/goe_mhealth_web.pdf (2015. 03. 22.)

zösségi élet) való használatra. A sávszélesség bővülése révén megjelentek új törekvések is az adatérzékeny monitorozó megoldások irányába.

A mobil egészségügyi alkalmazások jellemzően okostelefonra, és az erre különféle csatornákon keresztül (Bluetoothon, wifin vagy közvetlenül) csatlakozó eszközökre (szenzorok) épülnek. A szenzorok által gyűjtött adatok felhasználásával az mHealth alkalmazás lehetővé teszi a távmonitorozást, elemzést, akár javaslatokat is ad a betegnek. Az mHealth megoldás az egyéneket összekapcsolja az egészségügyi nagyrendszerekkel és szolgáltatásokkal, biztosítja a szolgáltatóknak, hogy az egyes betegek valós idejű adatait gyűjtse, összesítse, a betegek állapotának nyomon követése alapján pedig személyre szabott, közvetlen szolgáltatásokat nyújtson.^{21, 22}

Számtalan feltörekvő technológia, periféria és szenzor integrálható az mHealth alkalmazásokhoz, a jövő internetes (future internet) technológiái és a big data alapú megoldások még tovább bővíthetik a lehetőségeket. A dolgok internete (Internet of Things, IoT) koncepcióval kombinálva az mHealth még eredményesebb lehet, további új szolgáltatásokat valósíthat meg. Számos külső információforrás is integrálható a távmonitorozás adataihoz, kibővítheti az elemzési lehetőségeket. Ezáltal a hagyományos reaktív, tüneteken alapuló egészségügyi modellek új, megelőzésre törekvő megközelítésekkel válthatók ki. A modell nemcsak a betegellátás minőségét javítja, hanem olcsóbb is, mint a hagyományos, egészségügyi intézményekre épülő szolgáltatási modell. Ez a kórházközpontú szolgáltatási rendszerről az állampolgár-orientált, személyre szabott egészségügyi szolgáltatásokra való áttérést segíti elő. Időt takaríthat meg a beteg és az orvos is, a szektorszintű, aggregált adatok elemzése pedig a tendenciák feltárása révén a döntéshozóknak nyújthat segítséget.

West²³ 5 fő alkalmazási kategóriába sorolta be az mHealth szolgáltatásokat:

- közegészségügyi kutatások (egészségügyi adatok gyűjtése mobilhálózatokon),
- közvetlen gondozás a távoli erőforrások elérhetővé tételével,
- sürgősségi/vészhelyzeti szolgáltatások,
- hosszú távú gondozás támogatása rutin diagnosztika és ellenőrzések biztosításával,
- információ és önkiszolgáló segítség.

Az alkalmazások köre a mobilalapú előjegyzési rendszertől a gyógyszer-monitorozó és jogosultság-ellenőrző, a távoli diagnosztikai és életminőség-javító megoldásokon át a mobil telegondozásig terjed. Ez a cikk a negyedik kategóriával, a szenzorokkal kiegészített diagnosztikai megoldásokkal foglalkozik. Vizsgálatok szerint a betegek és az orvosok is számos előnyét élvezik a mobilalapú távmonitorozó rendszereknek, pl. bármilyen, az egészségi állapotot kedvezőtlenül befolyásoló tényező korai jeleinél gyors riasztás és azonnali segít-

21 Kyle Leon WEST: *mHealth: A Comprehensive and Contemporary Look at Emerging Technologies in Mobile Health*. Forrás: trace.tennessee.edu/cgi/viewcontent.cgi?article=2711&context=utk_chanhonoproj (2014. 08. 26.)

22 WHO: *mHealth: New horizons for health through mobile technologies: second global survey on eHealth*, 2011. (ISBN 978-92-4-156425-0) Forrás: www.who.int/goe/publications/goe_mhealth_web.pdf (2015. 03. 22.)

23 Kyle Leon WEST: *i. m.*, 2014. Forrás: trace.tennessee.edu/cgi/viewcontent.cgi?article=2711&context=utk_chanhonoproj

ségnyújtás lehetséges. Ugyanakkor számos feltétel és kérdés is megfogalmazható ezekkel a rendszerekkel szemben:²⁴

- a felhasználókat megfelelően ki kell képezni;
- ergonomikus tervezés kell a könnyű használhatóság érdekében;
- nem mindenki számára elérhető/alkalmas eszköz (látásproblémák, kézmozgással kapcsolatos nehézségek);
- az eszköz nem helyettesíti, inkább kiterjeszti a beteg és az orvos közti kapcsolatot;
- az alkalmazás nem okozhat jelentős munkateher-növekedést;
- a megvalósítás költsége nem lehet magas;
- a kockázatokat kezelni kell, elkerülendő pl. hogy a riasztási algoritmus téves jelzést vagy nem megfelelő tanácsot adjon;
- a betegek személyes adatait óvni kell;
- a jogi-szabályozási környezet még nem teljes mértékben kidolgozott.

2.2. Társadalmi-kulturális hatások

A társadalom szempontjából az mHealth számos előnyt kínál: csökkenti az egészségügyi ellátás költségeit, javítja annak minőségét, és elérhetővé teszi a szolgáltatásokat a fejletlenebb vagy nehezen megközelíthető helyek lakossága számára is. Másrészről rengeteg kérdés és aggály is megfogalmazható. Al Ameen és társai az mHealth számos problémáját vizsgálták, pl. személyiségi jogok, biztonság, jogi, gazdasági, pszichológiai és politikai kérdések.²⁵ Az mHealth infrastruktúra egyik kulcseleme a szenzorhálózat, ami sérülékeny összetevő, számos biztonsági fenyegetés kapcsolható hozzá. Több kutatás^{26, 27, 28, 29, 30} is elemzi a felsorolt problémákat.

Az okostelefonok elterjedése és az egészségvédelemmel kapcsolatos alkalmazások népszerűsége az mHealth társadalmi elfogadottságát nagyban elősegítik. Ezekkel a trendekkel

24 Emily SETO et al.: *Attitudes of heart failure patients and health care providers towards mobile phone-based remote monitoring*, Journal of Medical Internet Research, 12(2010)/4.

25 Al Ameen MOSHADDIQUE, Kyung Sup KWAK: *Social Issues in wireless sensor networks with healthcare perspective*, Int. Arab J. Inf. Technol., 8(2011)/1, 52–58.

26 Frank KARGL et al.: *Security, privacy and legal issues in pervasive ehealth monitoring systems*, Mobile Business, 2008, ICMB '08, 7th International Conference IEEE, 2008/296–304.

27 Marci MEINGAST, Roosta TANYA, Sastry SHANKAR: *Security and privacy issues with health care information technology*, 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS '06, Aug. 30–Sept. 3, 2006/5453–5458.

28 H. S. NG, M. L. SIM, C. M. TAN: *Security issues of wireless sensor networks in healthcare applications*, BT Technology Journal, 2006, Vol. 24. No. 2., 138–144.

29 Yong WANG, Attebury GARHAN, Ramamurthy BYRAV: *A survey of security issues in wireless sensor networks*, IEEE Communications Surveys & Tutorials, 2006, Vol. 8. No. 2., 2–23.

30 Zia TANVEER, Albert ZOMAYA: *Security issues in wireless sensor networks*, in Systems and Networks Communications, 2006, ICSNC '06, International Conference IEEE, 2006/40.

szemben viszont növekvő számban jelentek meg kifogások az okostelefonra írt alkalmazások pontosságával kapcsolatban, ami rontja a társadalmi elfogadást.³¹

A demográfiai trendek jelzik a 65 év feletti arányának növekedését, Magyarországon 2060-ra arányuk a teljes népességhez viszonyítva eléri a 29,5%-ot a 2013-as 17,4%-os arányhoz képest.³² Emiatt növekedni fog az egészségügyi szolgáltatások iránti igény is, ezzel párhuzamosan az idősek is egyre inkább igényelni fogják az önállóságot, az aktív részvételt egészségük fenntartásában.

Az életjelenségek (vérnyomás, szívverés, vércukorszint, súly, oxigénszint, ECG) távmonitorozása lehetővé teszi a krónikus betegek számára az önálló életvitelt, állapotuk alakulásának előrejelezhetőségét.³³

Az eHealth alkalmazásoknak jelentős a szociokulturális hatása is: pozitív és negatív módon is befolyásolhatják az embereket és a társadalmat, valamint a kulturális normákat. Egy tanulmány szerint³⁴ az eHealth és különösen az mHealth megoldások megfelelő eszközök lehetnek a harmadik világ egészségügyi kihívásaival kapcsolatban, ugyanakkor a tradicionális gyógyszerek és módszerek eltűnéséhez is hozzájárulhatnak.

Az Európai Unió (Európai Bizottság) 2004-ben fogadta el az első akciótervet³⁵ az eHealth széles körű alkalmazása érdekében, hiszen az mHealth hatékony eszköz lehet az idősödő társadalom és a növekvő költségvetési nyomás okozta problémák kezelésére, ugyanakkor komoly piaci potenciált is jelent az innovatív, új szolgáltatásokat nyújtó kvv-k számára. Az mHealth alkalmazások terjedése komoly potenciált jelent a big data irányú fejlesztések számára, másrészt nehezen kezelhető jogi-szabályozási problémákat vet fel a személyes adatok védelme, az alkalmazások engedélyeztetése és az egészségügyi tevékenységek értékláncában az egyéni és az intézményes feladatok megosztása terén; a biztonság és transzparencia, de pl. a finanszírozás is kulcsfontosságú kérdéskör.³⁶

A főbb jelenlegi (2012–2020 közti) időszakra vonatkozó célkitűzések az új akcióterv szerint:³⁷ – a krónikus megbetegedések hatékonyabb kezelése,

31 Joel WOLF et al.: *Diagnostic inaccuracy of smartphone applications for melanoma detection*, JAMA dermatology, 149(2013)/4, 422–426.

32 European Commission: *The 2015 Ageing Report*, 2015. (ISSN 0379-0991)

33 Fabienne ABADIE et al.: *Strategic Intelligence Monitor on Personal Health Systems (SIMPHS) Market Structure and Innovation Dynamics*, European Commission Joint Research Centre, Institute for Prospective Technological Studies. (ISBN 978-92-79-18947-0) Forrás: publications.jrc.ec.europa.eu/repository/bitstream/JRC62159/reqno_jrc62159_jrc62159.pdf

34 Jolene HUNTER, Richard E. SCOTT: *Considering the Socio-Cultural Impact of E-Health = Global Telehealth: Selected Papers from Global Telehealth 2010 (GT 2010): 15th International Conference of the International Society for Telemedicine and EHealth and 1st National Conference of the Australasian Telehealth Society*, IOS Press, 2010, Vol. 161., 77.

35 Európai Bizottság: *e-Health – making healthcare better for European citizens: An action plan for a European e-Health Area*, 2004. Forrás: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0356:FIN:EN:PDF (2014. 03. 23.)

36 Európai Bizottság: *GREEN PAPER on mobile Health*, 2014. Forrás: ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth (2014. 03. 23.)

37 Európai Bizottság: *eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century*, COM (2012) 736, 2012. Forrás: ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=9156 (2014. 03. 24.)

- az egészségügyi rendszerek fenntarthatóságának és hatékonyságának javítása,
- a betegközpontú ellátás fejlesztése,
- az ellátásokhoz való általános hozzáférés javítása,
- eHealth-termékek és szolgáltatások jogi és piaci feltételeinek fejlesztése.

Az aktuális megoldandó problémák közt kiemelt jelentőségű az interoperabilitás fejlesztése (a tagállamok eHealth-rendszereinek együttműködése, a folyamatok integrálhatósága), valamint a jogi akadályok leépítése (a felelősség, az engedélyezés és az adatvédelem kérdései, a határokon átvéelő szolgáltatások területén).

Az EU által támogatott fejlesztési projektek, kutatási irányok sorában számos betegség-típusra koncentrááló projekt indult, a mentális betegségektől, epilepsziától, Parkinson-kórtól kezdve a cukorbetegségen át a tüdő- és szívbetegségekig, a rákos megbetegedésekig minden fontosabb területen fejlesztenek innovatív megoldásokat. Az elmúlt években inkább a kis léptékű, egy-egy koncepció, részterület lehetőségeit feltáró „proof of concept” jellelő, vagy éppen innovációk alkalmazhatóságát validáló pilotfejlesztések voltak jellemzőek. A 2012–2020-as időszakban az integrált, fenntartható, ügyfélközpontú megoldások fejlesztése a meghatározó,³⁸ kiemelt terület a mobil- és testre szabott szolgáltatások fejlesztése, az interoperabilitás és szabványosítás.³⁹

2.3. Az e-egészségügyi megoldások gazdasági aspektusai

Az e-egészségügyi megoldások gazdasági szempontjainak vizsgálatakor a várható hasznokat kell összehasonlítani a fejlesztéshez kapcsolódó költségekkel. A bonyolultabb mHealth-alkalmazások költséges infrastruktúra kialakítását igénylik, ahol a már meglévő rendszerekkel való integráció egy újabb költségnövelő kihívás. Az mHealth-megoldások megfogható és nem megfogható hasznainak kiszámításakor elsődlegesen a hatékonyság növelésének időkímélő és költségelkerülő tényezőit érdemes figyelembe venni.

Lee és társai⁴⁰ a távmonitorozás költségsökkentési jellemzőit vizsgálták, elsődlegesen az emberi erőforrás (egészségügyi személyzet, nővérek és orvosok), valamint a beavatkozások számának csökkentése szempontjából. 486 szívbeteg adatainak felhasználásával egy olyan adatbányászati [SVM (Support Vector Machine) alapú] osztályozó modellt készítettek, amely a beavatkozások szükségességének előrejelzését támogatja. Ezt a megoldást hasonlították össze a „hagyományos” szabályalapú távmonitorozó rendszerekkel (az előrejelzés pontossága és gazdasági szempontok alapján). Elemzéseik szerint a vizsgált hathónapos időszakban megoldásukkal a beavatkozásokkal kapcsolatos költségek jelentős, 61,5%-os csökkenése érhető el.

38 Európai Bizottság: *GREEN PAPER on mobile Health*, 2014. Forrás: ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth (2014. 03. 23.)

39 Európai Bizottság (DG CONNECT): *eHealth projects – Research and Innovation in the field of ICT for Health and Wellbeing: an overview*, Publications Office of the European Union – Luxembourg, 2015. Forrás: ec.europa.eu/newsroom/dae/document.cfm?doc_id=2852 (2015. 12. 22.)

40 Sunghoon Ivan LEE et al.: *Remote patient monitoring: what impact can data analytics have on cost?* = Proceedings of the 4th Conference on Wireless Health, ACM, 2013.

Az e-egészségügyi megoldások egy további költségsökkentéssel kapcsolatos előnye, hogy a hosszabb időszakra rendelkezésre álló egészségügyi élettörténet miatt az egészségügyi tesztek nem szükségesek újra és újra elvégezni. Így az egészségügyi szolgálat és a betegek is időt és pénzt takaríthatnak meg (idetartozik az utazási költség megtakarítása is).^{41,42} Az egészségügyi szakemberek a rendelkezésre álló adatokból készített elemzésekkel testreszabottabb kezelést tudnak nyújtani, mint a hagyományos vizsgálat során, amikor csak egy adott időpontban, vagy időintervallumban ismertek a beteg egészségügyi adatai. A biztosítótársaságok a duplikált egészségügyi tesztek kizárásával szintén jelentős költségmegtakarítást érhetnek el, ahogyan azt Stroetmann és társai kimutatták.⁴³

Az mHealth-megoldások gazdasági jellemzőit vizsgálva, az okostelefonok és a kapcsolódó háttérrendszerek beszerzése és üzemeltetése jelent mind a betegek, mind az egészségügyi szolgáltatók számára jelentős költséget. Egy további költségnövelő tényező az egészségügyi adatokat gyűjtő és elemző viselhető készülékek beszerzése. Egyes páciensek továbbá úgy érezhetik, hogy ezek az eszközök a személyiségi jogukat sértik, és egyes betegek mindennapi életvitelében is problémát jelenthetnek. Ezeket a kérdéseket a későbbiekben ismertetett PISCES e-egészségügyi megoldás kapcsán teszteltük, de a mi vizsgálatainkban a betegeknél nem merültek fel ilyen problémák.

2.4. Adatbiztonság és a személyiségi jogok védelme – a jogi aspektusok

Ebben a részben az e-egészségügyi megoldások jogi aspektusait vizsgáljuk, elsődlegesen az adatbiztonság szempontjainak figyelembevételével. A jogi vonatkozású kérdéseket nem tárgyaljuk teljeskörűen (terjedelmi korlátok miatt), inkább néhány fontosabb kérdésre hívjuk fel a figyelmet. Az e-egészségügyi alkalmazások számos jogi természetű kérdést vetnek fel: ki garantálja az e-egészségügyi rendszerek által szolgáltatott javaslatok/diagnózis helyességét; ki felelős a rossz diagnózisért és az ügyfelek adatainak biztonságával kapcsolatosan előforduló hibákért? Különösen fontos ebből a szempontból a mobilhálózaton történő egészségügyi adatok továbbítása. Wolf és társai felhívják a figyelmet a diagnosztikai pontatlanságokra és a szabályozási hiányosságokra is.⁴⁴ Sok ezer e-egészségügyi alkalmazást használnak már, miközben a környezet adatvédelmi kontrolljai nem mindig kielégítőek. Az e-egészségügyi megoldásokkal kapcsolatosan az alábbi fontosabb biztonsági céloknak kell megfelelni: megbízhatóság, bizalmasság, hitelesség és a rendelkezésre állás.

41 Catherine KLERSY et al.: *Economic impact of remote patient monitoring: an integrated economic model derived from a meta-analysis of randomized controlled trials in heart failure*. European Journal of Heart Failure, 13(2011)/4, 450–459.

42 Jolene HUNTER, Richard E. SCOTT: *Considering the Socio-Cultural Impact of E-Health = Global Telehealth: Selected Papers from Global Telehealth 2010 (GT 2010): 15th International Conference of the International Society for Telemedicine and EHealth and 1st National Conference of the Australasian Telehealth Society*, IOS Press, 2010, Vol. 161., 77.

43 Karl A. STROETMANN et al.: *i. m.* Published by the European Commission. Forrás: ec.europa.eu/information_society/activities/health/docs/publications/eHealthimpactsept2006.pdf (2010. 10. 25.)

44 Joel WOLF et al.: *i. m.*, JAMA dermatology, 149(2013)/4, 422–426.

Az adatbiztonság és a személyiségi jogok védelme az e-egészségügy egyik legfontosabb területe, ahogyan azt a XIII. Egészségügyi Infokommunikációs Konferencia adatbiztonsággal foglalkozó szekciójában is kiemelték.⁴⁵ Olyan adatintenzív ágazatról van szó, amelyben az egészségügyi és a személyes adatok gyűjtése, tárolása és használata valósul meg. Kulcskérdés a funkcionalitás biztosításának és a biztonsági kockázatok kezelésének az egyeztetése, miközben a fentiekben felsorolt biztonsági céloknak is meg kell felelni. Az e-egészségügy szolgáltatásainak biztosításához adatokra, gyakran személyes adatokra van szükség, miközben ezekkel az adatokkal számos visszaélés történhet.

A visszaélések két fő típusa ebben az esetben is az aktív és a passzív támadás. A passzív támadás során az elkövető feltérképezheti az e-egészségügyi megoldáshoz tartozó architektúrát, vagy jogtalanul szerez meg és használ fel egészségügyi adatokat. Aktív támadás lehet a beteg adatainak módosítása és így hamis riasztás elérése, vagy a hálózati adatforgalom megbénítása.⁴⁶ A szenzorok (az e-egészségügyi alkalmazások kulcselemei) elleni lehetséges támadásokat négy főbb kategóriába sorolhatjuk:⁴⁷ adatmódosítás, megszemélyesítéses támadás (impersonation), lehallgatás (eavesdropping) és a replaying hálózati támadás. Meingast és társai⁴⁸ az adatokhoz való hozzáféréssel, adattárolással, az adatintegritás biztosításával kapcsolatos kihívásokat elemzik az e-egészségügyi megoldásokban. Olyan adatbiztonsággal kapcsolatos kérdésekre keresik a választ, mint az adatgazda szerepkör funkcionalitása, a biztosító, az orvos és az esetleges harmadik fél adatbiztonsággal kapcsolatos felelőssége. További kihívást jelent a betegségekre vonatkozó adatok megosztásában a betegek személyiségi jogainak biztosítása, különösen akkor, ha a betegség társadalmi előítéletekkel terhelt, pl. pszichiátriai betegségek. Gondoljunk a Germanwings 2015. márciusi légi katasztrófájára, ennek alapján felmerülhet, hogy egyes esetekben hasznos lehetne, ha a munkáltatók hozzáférhetnének dolgozóik betegadataihoz. A felhasználók idegenkedhetnek az e-egészségügyi eszközök alkalmazásától, az adataikkal való visszaélések miatt, attól is tarthatnak, hogy adataikat beleegyezésük nélkül harmadik fél, pl. ügynökség hasznosíthatja. Az egészségügyi adatokkal való visszaélés egy másik formája, amikor az adatokat a közösségi médiában hozzák nyilvánosságra. Külön kockázati kategóriát jelentenek az idős, rászoruló betegek, akiknek sok esetben az e-egészségügyi megoldások használata (pl. okostelefonokat alkalmazó rendszerek) is nehézséget okozhat.⁴⁹

Bár technológiai oldalról kielégítő megoldások állnak rendelkezésre, az adatvédelem sokszor mégsem kap kellő figyelmet. Gyakran az állampolgárok sem tudják, hogy hol milyen

45 IME Szerkesztőség: A XIII. Egészségügyi Infokommunikációs Konferenciáról jelentjük, 14(2015)/6, 44–49.

46 Frank KARGL et al.: *Security, privacy and legal issues in pervasive ehealth monitoring systems*, Mobile Business, 2008, ICMB '08, 7th International Conference IEEE, 2008, 296–304.

47 Al Ameen MOSHADDIQUE, Kyung Sup KWAK: *i. m.*, Int. Arab J. Inf. Technol., 8(2011)/1, 52–58.

48 Marci MEINGAST, Roosta TANYA, Sastry SHANKAR: *i. m.*, 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS '06, Aug. 30–Sept. 3, 2006/5453–5458.

49 Michael RIGBY: *Applying emergent ubiquitous technologies in health: The need to respond to new challenges of opportunity, expectation, and responsibility*, International journal of medical informatics, 2007, Vol. 76., 349–352.

adataik vannak tárolva, így önrendelkezési jogaik is sérülhetnek, ahogyan azt Keleti Artúr a XIII. Egészségügyi Infokommunikációs Konferencián kifejtette.⁵⁰

Meingast és társai vizsgálták az e-egészségügyi megoldásokat használó betegek személyi jogaival kapcsolatos kérdéseket is.⁵¹ Többek között arra keresték a választ, hogy a betegek egészségügyi adatai milyen feltételek mellett tárolhatók és adhatók tovább. Kargl és társai⁵² felhívják a figyelmet arra, hogy az egészségügyi adatok személyes adatok is egyben, de a nem megfelelő adatbiztonság miatt könnyen publikussá válhatnak. A szerzők az e-egészségügyi megoldások biztonsági hiányosságainak következményeit is bemutatják. Az egészségügyi adatok nyilvánosságra hozása komoly hátrányokkal járhat az érintett beteg számára; pl. elveszítheti a munkáját, megszüntethetik a biztosítását, túl az egyéb, nehezen számszerűsíthető hátrányokon.⁵³

Madarászné részletes áttekintést ad a magyar szabályozási környezetről, a közigazgatási szervek egészségügyi adatkezeléséről. Rámutat arra is, hogy napjainkban a közigazgatás heterogén rendszerébe is kerülnek egészségügyi adatok, ahol nincsenek a jogszabályokban arra vonatkozóan korlátok, hogy ki ismerheti meg ezeket az adatokat.⁵⁴ Az egészségügyi adatok kezeléséhez a szabályozási környezet számos eleme kapcsolható, a fontosabbak:

- Magyarország Alaptörvénye VI. cikk (2): Mindenkinnek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez,
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
- az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról [megújítása folyamatban van, 2015. december 18-án egy megújított változatot (általános adatvédelmi rendelet⁵⁵) hagytak jóvá],
- az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény,
- az Európai Parlament és a Tanács 2002/58/EK Irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről („Elektronikus hírközlési adatvédelmi irányelv”),
- az 1997. évi CLIV. törvény az egészségügyről,
- az 1997. évi LXXXIII. törvény a kötelező egészségbiztosítás ellátásairól.

50 IME Szerkesztőség: A XIII. Egészségügyi Infokommunikációs Konferenciáról jelentjük, 14(2005)/6, 44–49.

51 Marci MEINGAST, Roosta TANYA, Sastry SHANKAR: *i. m.*, 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS '06, Aug. 30–Sept. 3, 2006, 5453–5458.

52 Frank KARGL et al.: *Security, privacy and legal issues in pervasive health monitoring systems*, Mobile Business, 2008, ICMB '08, 7th International Conference IEEE, 2008, 296–304.

53 Kumar PARDEEP, Hoon-Jae LEE: *Security issues in healthcare applications using wireless medical sensor networks*, A survey, Sensors, 2011, Vol 12. No. 1., 55–91.

54 MADARÁSNÉ IFJU Bernadett: *A közigazgatási szervek egészségügyi adatkezelése*, Pro Publico Bono – Magyar Közigazgatás, 2014, Vol. 4., 170–184.

55 Forrás: www.consilium.europa.eu/hu/press/press-releases/2015/12/18-data-protection/

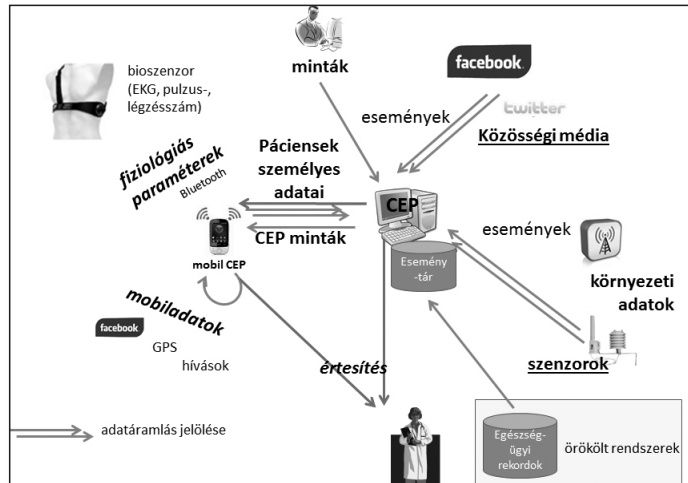
3. A PISCES TUDÁSALAPÚ, TÁVMONITOROZÓ MEGOLDÁS (RESPONSIVE HEALTH MONITORING SOLUTION)

Ebben a részben áttekintést adunk a PISCES eHealth megoldásról, amelyet az EUREKA_HU_12-1-2012-0007 – PISCES – Future Internet megoldások támogatása az egészségügyben (CPP2011/1-3 – PISCES – Promoting Future Internet Solutions in Health Environments) projektben fejlesztettünk ki, a Jövő Internet Paradigmája (Future Internet Paradigm) koncepciójához illeszkedően. A PISCES projekt célja olyan alkalmazások létrehozása volt, amelyek a krónikus betegek állapotának és életkörülményeinek részleges monitorozásával hozzáadott értékű szolgáltatásokat nyújtanak a felhasználóknak. A PISCES-megoldás tudásalapú, intelligens távmonitorozást megvalósító mobiltechnológiára épülő rendszer. Támogatja a páciens egészségügyi állapotának távoli ellenőrzését, figyelembe véve a páciens tevékenységét és a környezeti hatásokat is (időjárással és egyéb a környezettel kapcsolatos tényezők, pl. légszennyezettség). A PISCES-megoldás az egészségügyi állapot monitorozásán túl segít az irreguláris események azonosításában és a hozzájuk kapcsolódó akciók megtervezésében is.

A PISCES rendszer innovatív jellegét elsődlegesen az ún. Complex Event Processing (CEP) algoritmusok alkalmazása biztosítja. A CEP segíti a páciensek egyes élettani változói (pl. szívritmus, EKG, fizikai aktivitás stb.), illetve környezeti változók (külső hőmérséklet, légnyomás, páratartalom stb.) bonyolult rendszere és az ebből levonható egyes következtetések közötti kapcsolat megteremtését. A következtetéseknek két típusa van, lehetnek azonnali riasztások vagy egy hosszabb vizsgált időszak eseményei alapján megállapítható események.

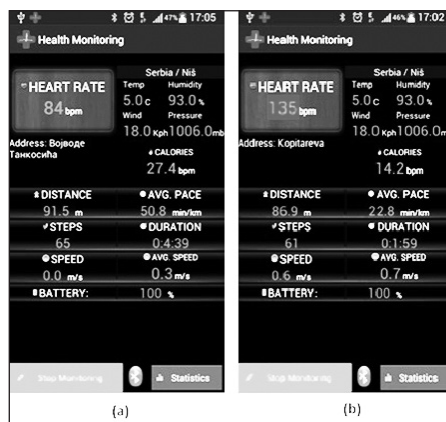
A fejlesztést nemzetközi konzorcium végezte, amelynek több szakaszában részt vettünk a koncepció kialakításától a tesztelésig. Az 1. ábra mutatja a PISCES-megoldás főbb részeit és a közöttük történő adatcserét. A rendszernek három főbb, funkcionálisan elkülönülő része van: a mobil eszközre és a szenzorokra támaszkodó adatgyűjtő komponens; az adattároló komponens és az egészségügyi szempontok figyelembevételével kialakított megjelenítő, vizualizációs komponens. A rendszer egyik központi eleme a mobil szenzor (okostelefon és a páciens által viselt szenzor). A páciens által viselt szenzor egy ún. bioszenzor, egy wireless pulzus-, légzésszám-, EKG-monitor, valamint a fiziológias paraméterek észlelésére alkalmas készülék. Ez a berendezés rögzíti és tárolja a mért adatokat, és képes azokat egy külső adatfogadó készülék (okostelefon) felé továbbítani.

1. ábra • A PISCES-megoldás⁵⁶



A háttérrendszer főbb részei a CEP-szerver és a Context Management Framework. A háttérrendszer fő funkciója az adatok elemzése és ennek alapján üzenetek és riportok küldése az érintetteknek (egészségügyi szakembereknek és a pácienseknek). Az egészségügyi szakemberek (orvosok és nővérek) számára további elemzési lehetőségeket nyújt a PISCES portál, amelyen keresztül egy adott időszakhoz tartozó adatok lekérdezhetők, elemezhetők, a riasztási eseményekkel együtt. A CEP-szerver felelős a külső forrásokból történő adatgyűjtésért (pl. közösségi média vagy időjárás adatok) is, továbbá kapcsolatot tart a szakterületi tudásbázisokkal. A páciens az okostelefonon keresztül kap visszajelzést egészségügyi állapotáról (2. ábra).

2. ábra • A PISCES-riport mobilon



56 GÁBOR András: PISCES – Responsive Remote eHealth = Proceedings of 8th International Conference on Software, Knowledge, Information Management and Applications, 2014, 199.

A PISCES-megoldást Magyarországon két helyszínen, a Kelen Kórházban és a Honvédkórházban tesztelték 2014 áprilisa és szeptembere között. A teszt résztvevői szívélégtelenségben szenvedő betegek voltak, akik egyenként egy hétig viselték folyamatosan a testre helyezhető szenzort. A mérési eredmények tanúsága szerint a betegek nagyobb százaléka a teljes 24 órából, az alvási időt nem számítva, az idő 50-60%-ában tartotta bekapcsolva az alkalmazást. A gyűjtött adatok csoportjai:

- szenzor által mért pulzus, légzésszám, EKG,
- az okostelefon által automatikusan rögzített mozgásadatok és helymeghatározási adatok;
- az azonos időszakhoz tartozó meteorológiai adatok: hőmérséklet, páratartalom, légnyomás, szélerősség, és
- a betegek által rögzített értékek: vérnyomás, testsúly, alkoholfogyasztás, dohányzás.

A teszt során a PISCES-rendszerrel kapcsolatosan az alábbi fontosabb visszajelzések érkeztek:

- az eszközök hálózatfüggetlen (akkumulátor) tápellátása nem kielégítő, csak 4-6 órára elegendő;
- az okostelefon használata, kezelése nehézségekbe ütközik idősebb korban – az alkalmazás felhasználói felületének áttervezése (egyszerűsítése) után ezek a panaszok csökkentek;
- a betegek szubjektív megítélése szerint a szenzor viselése nem okozott különösebb nehézséget vagy kényelmetlenséget, ezzel szemben fokozta biztonságérzetüket;
- adatminőségi problémák csak abban az esetben voltak észlelhetők, amikor a szenzorok elhelyezése nem volt megfelelő.

Ahhoz hogy a PISCES eHealth-megoldást a gyakorlatban széleskörűen is alkalmazni lehessen, az előző pontokban tárgyalt gazdasági, szabályozási, adatbiztonsági, társadalmi és kulturális szempontok elemzése is szükséges.

4. KONKLÚZIÓ

A PISCES-megoldás a magyar teszt eredménye szerint eredményesen és hatékonyan működtethető. A legfontosabb hozzáadott érték a felhasználói profilok automatikus kialakítása és az automatikus riportolási funkció. Ez utóbbi teszi lehetővé a riasztások esetében a valós idejű adatfeldolgozás segítségével a beavatkozást, illetve a felhasználói visszajelzés küldését. Az adatfeldolgozást a nagy adatmennyiségek elemzését lehetővé tevő funkciók is támogatják. A kontextus leírása és kezelése szemantikus technológiák alkalmazásával történik. Informatikai szempontból az egyik fontos visszajelzés a felhasználók részéről az egyszerűbb, átláthatóbb és hatékony keresőkkel ellátott portálok iránti igény megfogalmazása volt. A projektben alkalmazott megközelítés jól hasznosítható viszonylag ritkán jelentkező szívritmuszavarok felismerésére, a beteg ugyanis meg tudja jelölni az adathalmazban azt az időszakot, amikor nem érezte jól magát. A PISCES-megoldás valós idejű egészségügyi adatok (fiziológiai paraméterek, pl. frekvencia, légzésszám, EKG-adatok) gyűjtését teszi lehetővé. Az adatok felhasználhatók a rendszer által automatikusan szolgáltatott paraméterekkel (pl. mozgásparaméterek, meteorológiai adatok) történő összevetésre, és a kezdeti adatgyűj-

tési időszak után helyzetre és személyre szabott riasztási értéket lehet beállítani. A pilot alapján kifejleszhető alkalmazás lehetővé teszi nagyszámú beteg távmonitorozását és így a fiziológiai paraméterek kóros változásának észlelését. Mindez jelentősen csökkentheti az orvos-beteg találkozások számát, és a kórházi felvételek száma is csökkenthető. A nagyobb biztonságérzet és a javuló mozgásszabadság is javíthatja a betegek életminőségét. Szektorszinten egy ilyen megoldás csökkentheti az ellátórendszer túlterheltségét és az ellátás költségeit.⁵⁷

A PISCES-megoldás egy lehetséges továbbfejlesztése a további szenzorokkal és alkalmazásokkal történő kiegészítés. További jövőbeli kutatási irány lehet formális keretrendszerek és eljárások alkalmazási lehetőségeinek vizsgálata a PISCES-architektúra hatékonyságának javítására.⁵⁸ A PISCES alkalmazás igazolta, hogy a jövő internetes technológiai és a szemantikus technológiák jól támogatják a testre szabott egészségügyi szolgáltatások kialakítását. Az eHealth és mHealth alkalmazások a korszerű informatikai megoldásokkal kiegészítve jelentősen hozzájárulhatnak az egészségügyi prevenció szolgáltatások kialakításához és menedzsmentjéhez. Ahhoz, hogy ezeket a megoldásokat operatíván is alkalmazni tudjuk, figyelembe kell vennünk a gazdasági, szabályozási, adatbiztonsági, társadalmi és kulturális szempontokat is, ahogyan arra a fentiekben rámutattunk. Ebben az esetben az eHealth és mHealth alkalmazások jól kiegészíthetik a jelenleg is működő egészségügyi szolgáltatásokat.

KÖSZÖNETNYILVÁNÍTÁS

A cikket és a kutatást a PISCES – Promoting Future Internet Solution Health Environment projekt (EUREKA_HU_12-1-2012-0007) támogatta, a Corvinno Technology Transfer Center Kft. részvételével. Külön köszönjük Dr. Nenad Stojanovicnak a rendszer kifejlesztéséhez nyújtott támogatását.



SUMMARY IN ENGLISH: The healthcare industry, especially in Central and Eastern European countries, is facing several challenges nowadays, like aging population, “doctor exodus”, and financing problems. For this reason, we must pay particular attention to the prevention and monitoring of patients’ health-status. eHealth is a key priority of “Egészségügyi Ágazati Stratégia 2015” in Hungary. eHealth, mHealth and Future Internet solutions provide high-quality health services, which can be utilized to move far beyond traditional care. New, innovative services are offered, like remote health monitoring, which provide cost effective solutions in a relative low cost infrastructure. This paper discusses social, economic, security, privacy and legal perspectives of eHealth solutions and we present PISCES, a responsive health monitoring mobile information system, which enables remote monitoring of the patients’ health-status.

57 LUKÁCS Imre, NYOLCZAS Noémi: *Beszámoló a PISCES vizsgálatról*, 2015/12.

58 MOLNÁR Bálint, BENCZÜR András: *Facet of Modeling Web Information Systems from a Document-Centric View*, International Journal of Web Portals (IJWP), 5, 4, IGI Global, 2013, 57–70.

Dr. Kő Andrea, PhD, Habil, CISA (ko@informatika.uni-corvinus.hu): egyetemi docens a Budapesti Corvinus Egyetem Információrendszerek tanszékén. Programigazgató a Budapesti Corvinus Egyetem Gazdaságinformatika Doktori Iskolájában. Számos nemzetközi és hazai kutatási projektben vett részt a tudásmenedzsment, a szemantikus technológiák, az e-kormányzat és az infokommunikációs technológiák alkalmazásainak különböző területein. Több mint 90 közleményt publikált folyóiratokban, könyvekben és konferenciakötetekben. Főbb kutatási területei: szemantikus technológiák, ontológiák alkalmazási lehetőségei, üzleti intelligencia, intelligens rendszerek, tudásmenedzsment.

Dr. Szabó Zoltán, PhD (szabo@informatika.uni-corvinus.hu): egyetemi docens a Budapesti Corvinus Egyetem Informatikai Intézetében, az Információrendszerek tanszék vezetője. 1994-ben szerzett közgazdász diplomát, majd 2001-ben kapott PhD-fokozatot a Gazdálkodástudományi Doktori Iskolában. Kutatási területei: folyamatmenedzsment, informatikai stratégiatervezés, stratégiai összehangolás, IT-szolgáltatás-menedzsment, e-kormányzat, vállalatiarchitektúra-menedzsment. ITIL manager (1997) majd ITIL expert (2009) minősítéssel rendelkezik. Több mint 40 tudományos közleménye jelent meg nemzetközi és hazai folyóiratokban, konferenciakötetekben. Számos nemzetközi és hazai kutatási, ill. K+F projekt résztvevője tudásalapú rendszerek, e-kormányzati, mHealth, SBPMN, ITSM témákban.

AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATELEMZÉS MÓDSZERTANI KÉRDÉSEI A KRITIKUS INFRASTRUKTÚRA ELEMÉKET ÜZEMELTETŐ SZERVEZETEK ESETÉBEN

A létfontosságú rendszerek üzemeltetése során is egyre nagyobb szerep hárul a mind komplexebb informatikai rendszerekre. A térhódítással együtt jár a kockázatok számának, a rendszerek sérüléséből eredő károk mértékének ugrásszerű növekedése. Ma már egyetlen szervezet működéséből sem hiányozhat az információbiztonsági tevékenység. Különösen igaz ez a kritikus infrastruktúra rendszereket üzemeltető szervezetek esetében, ahol jogszabályok is rögzítik az információbiztonsági tevékenység kereteit és elvárásait.

Ennek tükrében – gyakorlati tapasztalatainkat is felhasználva – mutatjuk be az információbiztonsági kockázatmenedzsment tevékenység folyamatának egy olyan lehetséges kialakítását, amely egyszerre veszi figyelembe a szabványok elvárásait, valamint a vonatkozó jogszabályi követelményeket. Véleményünk szerint a két követelményrendszer megfelelően harmonizálható, a szervezet adottságait is figyelembe vevő működési keret alakítható ki, mely nagymértékben képes növelni a szervezet biztonsági szintjét.

KULCSSZAVAK:

biztonsági osztályok, CIP, IBIR, interdependencia, ISO/IEC 27 000, létfontosságú rendszer, vagyonelemek



1. BEVEZETÉS

A létfontosságú rendszerekről és létesítményekről szóló törvény¹ (Lrtv.), valamint hozzá kapcsolódóan, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény² (Ibtv.) rengeteg feladatot ró a kritikus infrastruktúrát üzemeltető szervezetekre. Az állami törekvések hatásaként a kritikus infrastruktúrák üzemeltetésében várhatóan

1 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

egyre nagyobb szerep hárul különböző állami intézményekre, vállalatokra.³ Ezen túlmenően a létfontosságú ágazatok közé tartozik a jogrend, kormányzat, valamint a közbiztonság, védelem területe is. A létfontosságú rendszereket üzemeltető szervezetek jelentős része működése során alkalmaz valamilyen (akár több) irányítási rendszert, ugyanakkor a közigazgatás területén is kezdenek megjelenni a különböző irányítási rendszerek.⁴ Az információbiztonság területén széles körben alkalmazott az ISO/IEC 27001-es szabvány szerinti információbiztonsági irányítási rendszer (IBIR).⁵

A kritikus infrastruktúra rendszerek működése és védelme a társadalom működése szempontjából kiemelt jelentőséggel bír, ugyanakkor a kockázatokkal arányos és költséghatékony védelem kialakításának elengedhetetlen eszköze a kockázatmenedzsment. Munkánkban azt mutatjuk be, hogy tapasztalataink alapján milyen módon lehet a gyakorlatban kialakítani és megvalósítani az ISO/IEC 27000 szabványcsaládnak teljes mértékben megfelelő, a gyakorlatban jól használható módszertant kritikus infrastruktúrákat üzemeltető szervezetek esetében. A következőkben egy az ISO/IEC 27001 szabványnak megfelelő információbiztonsági kockázatmenedzsment-szabályzat kialakítását mutatjuk be, mely figyelembe veszi a kritikus infrastruktúra üzemeltetőkre vonatkozó jogszabályi követelményeket. Megvizsgáljuk a felmerülő kérdéseket, problémákat, és bemutatunk egy lehetséges megoldást is.

2. A KRITIKUS INFRASTRUKTÚRÁK JELLEMZŐI

A modern társadalmak működéséhez elengedhetetlenül szükség van különböző infrastruktúrák szolgáltatásaira, melyek folyamatosan biztosítják az emberek életének és a gazdaság működésének feltételeit. Ilyen infrastruktúra lehet például az energiaellátás, az infokommunikáció, a közlekedés, de a pénzügyi rendszer is. Könnyen belátható, hogy a felsoroltak közül bármelyik elégtelen működése komoly károkat okoz a társadalom számára, így ezen infrastruktúrák kielégítő működése kritikus fontosságú.

2.1. Jogszabályi környezet

A kritikus infrastruktúráknak (létfontosságú rendszerek) számos meghatározása létezik.^{6,7} A katasztrófavédelemről szóló kormányrendelet⁸ a következő definíciót tartalmazza:

3 BÁLINT Norbert et al: *A közösségi közműszolgáltatás megszervezésének egyes szabályozási kérdéseiről*, Pro Publico Bono – Magyar Közigazgatás, 3(2015)/1, 4–18.

4 Soós Hajnalka: *Szemelvények a minőségbiztosítási rendszerek megjelenéséről*, Pro Publico Bono – Magyar Közigazgatás, 1(2013)/3, 121–124.

5 MICHELBERGER Pál és LÁBODI Csaba: *Vállalati információbiztonság szervezése = Vállalkozásfejlesztés a XXI. században II.*, szerk. NAGY Imre Zoltán, Óbudai Egyetem, Budapest, 2012, 241–302.

6 USA PATRIOT Act (H.R. 3162)

7 COM(2006) 787 final 2006/0276 (CNS), Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection

8 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról, 25. bekezdés

„Kritikus infrastruktúra: Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.”

Az Lrtv. pedig a következő definíciót használja:

„Létfontosságú rendszerelem: az 1–3. mellékletben meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyónbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.”

A mellékletben meghatározott tíz ágazat – valamint az utolsó két ágazat esetében az alágazatok is – a következő:

- Energia
- Közlekedés
- Agrárgazdaság
- Egészségügy
- Pénzügy
- Ipar
- Infokommunikációs technológiák
- Víz
- Jogrend – Kormányzat
 - kormányzati rendszerek, létesítmények, eszközök
 - közigazgatási szolgáltatások
 - igazságszolgáltatás
- Közbiztonság – Védelem
 - rendvédelmi szervek infrastruktúrái
 - honvédelmi rendszerek és létesítmények

Azon szervezeteknek, melyek kritikus infrastruktúrát üzemeltetnek, be kell tartaniuk az Ibtv.-t, valamint a hozzá kiadott végrehajtási rendeletet⁹ (vhr.), mely a szervezet informatikai rendszerével kapcsolatos követelményeket tartalmaz.

A felsoroltakon kívül természetesen még rengeteg jogszabályhoz kell alkalmazkodnia a szervezeteknek, azonban az ismertetett jogszabályok az elsődleges források a szabályzat kidolgozása során.

9 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről, majd 2015. július 17-től pedig 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

2.2. Interdependencia

Az egyes infrastruktúrák működtetéséhez szükség van más infrastruktúrák igénybevételére. Az infokommunikációs technológiák (IKT) fejlődésének következtében szerepük kiemelkedő fontosságú, aminek oka, hogy szinte minden infrastruktúra üzemeltetéséhez elengedhetetlenül szükséges a megfelelő működésük. A magyarországi távközlési és energetikai szektor bevonásával¹⁰ végrehajtásra került kritikus infrastruktúra védelmi gyakorlat szintén rámutatott az IKT-ágazat kiemelt fontosságára. Ráadásul az ipari automatizálási rendszerek (Supervisory Control and Data Acquisition, SCADA) elterjedésével olyan informatikai eszközök kerültek alkalmazásra, melyek tevékenységük során fizikai beavatkozó eszközöket irányítanak, mint például a jelzőlámpák, vasúti váltóberendezések, szivattyúk, repülőgépek, atomerőművek, de akár fegyverrendszereket is. Az informatikai rendszerek komplexitásának növekedése pedig egyre nagyobb kockázatot megjelenését idézte elő.¹¹ A kritikus infrastruktúrák kölcsönös függőségét Rinaldi és társai,¹² valamint Dudenhoeffler és társai¹³ vizsgálták részletesen. Az IKT kiemelkedő jelentőségét mutatja az is, hogy bevezetésre került a kritikus információs infrastruktúrák fogalma. A 2005. november 17-én elfogadott, a „Létfontosságú infrastruktúrák védelmére vonatkozó európai programról szóló „Zöld könyv”¹⁴ 1-es melléklete a kritikus információs infrastruktúrákat a következőképpen azonosítja: „Kritikus Információs Infrastruktúra (CII): IKT-rendszerek, melyek önmagukban kritikus infrastruktúrák, vagy létfontosságúak kritikus infrastruktúrák működéséhez.”¹⁵

Mindezek alapján különösen fontos az informatikai rendszerek megfelelő kockázatmenedzsment-folyamatának kialakítása.

2.3. Kritikus infrastruktúra üzemeltető szervezetek jellemzői

A kritikus infrastruktúrát működtető szervezetek általában nagyvállalatok vagy jelentős állami intézmények. Működésük jól szabályozott, sokszor folyamatalapú, rendelkeznek a speciális ágazati tudást hordozó szakembergárdával és kialakult vállalati kultúrával. Általában saját informatikai infrastruktúrát építenek ki és biztosítják a hozzá megfelelő belső üzemeltetési erőforrásokat. Sok, ebbe a körbe tartozó szervezet már korábban is megfelelt az ISO/IEC 9001, valamint az ISO/IEC 27001 szabvány elvárásainak. Néhányuk pedig működését rendszeres auditok során tanúsította is. Fontos változás, hogy megjelent az ISO/IEC 27001

10 ANGYAL Zoltán, MAROS Dóra: *A távközlési és energiaszektor infrastruktúráinak interdependenciái, a 2010 KIV gyakorlat tapasztalatai = 17. HTE Infokommunikációs Hálózatok és Alkalmazások Konferencia és Kiállítás (Intelligens infrastruktúrák és alkalmazások)*, HTE, Siófok, 2010. 10. 27–2010. 10. 29, 34–45.

11 RAJNAI Zoltán, PUSKÁS Béla: *The risks of network complexity*, Bolyai Szemle, 33(2014)/2, 60–66.

12 Steven M. RINALDI et al.: *Identifying, understanding and analyzing critical infrastructure interdependencies*, IEEE Control Systems Magazine, 21(2001)/6, 11–25.

13 Donald D. DUDENHOEFFLER et al.: *CIMS: A framework for infrastructure interdependency modeling and analysis = WSC 06. Winter Simulation Conference*, IEEE, Monterey, 2006, 478–485.

14 Green Paper on a european programme for critical infrastructure protection (COM/2005/0576 final) Forrás: eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576 (2015. 12. 30.)

15 Saját fordítás.

szabvány első revíziója, az ISO/IEC 27001:2013, majd magyar szabványként az MSZ ISO/IEC 27001:2014. Az új szabvány beépítette az eddigi tapasztalatokat, valamint átstrukturálásra is került.

Az ISO/IEC 27005:2011 Information security risk management szabvány az ISO 27001 elvárásai alapján történő kockázatmenedzsmenttel kapcsolatban ad iránymutatásokat.

3. INFORMÁCIÓBIZTONSÁGI KOCKÁZATKEZELÉS

A kritikus infrastruktúra elemeket üzemeltető szervezetek valamilyen szinten formalizált Információbiztonsági Irányítási Rendszert (IBIR) működtetnek. A megváltozott körülmények és a megszerzett tapasztalatok szükségessé teszik az IBIR rendszer folyamatos értékelését és fejlesztését, melynek keretében az információbiztonsági kockázatkezelési tevékenység is zajlik. Általánosnak mondható, hogy Információbiztonsági Szabályzattal valamennyi szervezet rendelkezik, ugyanakkor az információbiztonsági kockázatkezelési szabályzat nem, vagy nem megfelelő minőségben áll rendelkezésre.

3.1. Az információbiztonsági kockázatkezelési szabályzat

Az információbiztonsági kockázatkezelési szabályzat kidolgozását (átdolgozását) egy erre dedikált projekt keretén belül célszerű megvalósítani.

A projekt résztvevői:

- az információbiztonságért felelős szervezet szervezeti egység-vezetője (célszerűen a projektszponzor),
 - az információbiztonságért felelős személy (a projekt vezetője),
 - az informatikai terület képviselője,
 - a szervezet általános (pénzügyi) kockázatkezelési területének képviselője,
 - a szervezet szabályozási területének képviselője,
 - amennyiben a szervezet nem rendelkezik a megfelelő szakmai kompetenciával (pl. CISA), akkor célszerű külső erőforrás bevonása is – akár tanácsadóként, akár minőségbiztosítóként.
- A projekt működésének támogatását adminisztratív eszközökkel is biztosítani kell:
- projektalapító dokumentum kidolgozása,
 - projektértekezletek,
 - változáskezelés stb. a szervezet projektkultúrájának megfelelően.

A projekt információbiztonsági vonatkozásai miatt különösen fontos a résztvevők közti biztonságos elektronikus kommunikáció megoldása, ezért titkosított megoldások (pl. SMIME, HTTPS) alkalmazása javasolt.

A szabályzat kidolgozása során, a folyamat egyes lépéseinek meghatározásához javasolt az ISO/IEC 2700X szabványcsalád, ezen belül is kiemelten az ISO/IEC 27001:2013 szabvány elvárásait figyelembe venni – még abban az esetben is, ha a szervezet nem tervezi a szabványnak való teljes megfelelést és ennek auditálását. A szakmai részletek kidolgozásánál pedig – mint erre a későbbiekben majd rámutatunk – célszerű a 2013. évi L. törvény és a hozzá tartozó végrehajtási rendelet elvárásait ötvözni, hiszen így biztosítható majd az elvárásoknak való megfe-

lelés. Ezen túlmenően, a folyamatos fejlődés érdekében, a PDCA modell alkalmazásához szükséges az eddigi tapasztalatok, valamint auditok megállapításainak, észrevételeinek beépítése is.

Arra kell törekedni, hogy az információbiztonsági kockázatkezelési szabályzat – és így végső soron maga az információbiztonsági kockázatkezelési tevékenység – megfeleljen az alábbi követelményeknek:

- a kockázatkezelési tevékenység a szervezet által meghatározott kereteken belül, a biztosított erőforrásokkal folyamatszerűen végezhető;
teljes mértékben lefedi a kockázatfelmérés és -kezelés folyamatát:
 - kockázatfelmérés,
 - kockázatértékelés,
 - kockázatkezelés,
 - kockázatelfogadás,
 - kockázatismertetés (kommunikáció),
 - követés és fejlesztés;
- a szabályzat alapján a kockázatfelmérés egyértelműen elvégezhető és bármikor reprodukálható, illetve aktualizálható,
- a kockázatok kezelésére meghatározott intézkedések hatékonyabb, kockázatarányos információbiztonsági kockázatkezelési tevékenységet tesznek lehetővé.

3.2. Az információbiztonsági kockázatkezelés folyamata

3.2.1. Biztonsági osztályok kialakítása

Az Ibtv. vhr.-je sok esetben meghatározza az új információbiztonsági kockázatkezelési szabályzat tartalmát, hiszen a jogszabályi megfelelés minden esetben elsődleges szempont. A jogszabály 1. Általános irányelvei is említik, hogy a kritikus infrastruktúrák esetében a rendelkezésre állás a legfontosabb szempont. Ugyanakkor azt is fontos megemlíteni, hogy a jogszabály sok kérdés esetében a döntést (vagy a pontosítást, vagy a konkrét megoldást) a szervezetre bízta. A biztonsági osztályok meghatározásánál is így járt el, ahhoz csak irányelveket fogalmaz meg, így lehetővé teszi a szervezet számára fontos szempontok alkalmazását is. Az osztályba sorolás szempontjai elsődlegesen az Ibtv. vhr. és a szervezet kockázatkezelési szabályzata alapján kerülhetnek kialakításra. Mindkét forrásból figyelembevételre kerülhetnek a lényeges szempontok, célszerű összerendelni az egyes kárérték-kategóriákat az egyes biztonsági osztályok összehatáraival. A káresemények mértékének meghatározása során az adattípusokhoz és adatmennyiségekhez elsődlegesen a jogszabály, míg az összehatárokhoz elsődlegesen a vállalati kockázatkezelési szabályzat szolgálhat forrásként.

A biztonsági osztályok kialakításánál fontos szempontok a következők:

- a vhr. 5. osztályt határoz meg a rendszerek biztonsági osztályba sorolásához;
- a szervezet létfontosságú rendszerelemeket üzemeltet;
- a szervezet általános kockázatkezelési gyakorlata;
- a szervezet pénzügyi mutatószámai;
- milyen típusú adatokat kezel a szervezet;

- milyen mennyiségben kezeli az adott adatokat;
- milyen forrásokból jut az adatokhoz;
- kiknek továbbítja az adatokat.

3.2.2. Információs vagyonelemek meghatározása

A szervezeti keretek definiálása után következő lépésként azonosítani kell azon adatforrásokat, melyek alkalmazhatók az információs vagyonelemek felmérése során. A szervezetek (tevékenységükből és méretükből adódóan is) számtalan nyilvántartással rendelkeznek, melyek általában sajnos nincsenek összekötve, integrálva, nem egységesek és csak manuálisan hozhatók kapcsolatba egymással. Nagyon fontos szempont, hogy a vagyonelemek felmérését rendszeresen el kell végezni, annak kellően pontosnak, részletesnek kell lennie, hogy elősegítse a kockázatmenedzsment feladatának elvégzését. Mindemellett a legtöbb szervezet nem használ az információbiztonsági kockázatmenedzsment feladatának elvégzésére automatizált eszközöket, így célszerűen olyan módszertan kerülhet kidolgozásra, mely az információs vagyonelemek azonosítását csak olyan részletességgel végzi el, mely feltétlenül szükséges.

Az információs vagyonelemek azonosítása során két lehetséges megközelítés merül fel. Az első módszer esetében alulról építkezve, az összes vagyonelem összegyűjtése a különböző nyilvántartásokból, majd azoknak folyamatokhoz rendelése történik meg bottom-up módon. Ez lényegesen pontosabb, minden részletre kiterjedő azonosítást eredményezhet, azonban nagyon sok energiát igénylő feladat. A második megoldás esetében top-down módon, első lépésként az üzleti folyamatok kerülnek azonosításra, majd ezt követően az egyes folyamatokhoz a folyamatokban részt vevő vagyonelemek azonosítása történik meg. Ez a megoldás alacsonyabb erőforrás-ráfordítással elvégezhető, azonban a nem azonosított információs vagyonelemek aránya magasabb lehet, mint az első módszer esetében.

Külön hangsúlyoznunk kell, hogy a nyilvántartások rendelkezésre állása és tartalmuk minősége nagymértékben meghatározza a teljes kockázatkezelési tevékenység minőségét. Abban az esetben, ha a kockázatkezelési projekt keretében kell elvégezni felméréseket, leltározásokat, az adatok aktualizálását és tisztítását, akkor az eredetileg becsült erőforrás- és időszükséglet valószínűleg többszörösére nő. A megfelelő megközelítés kiválasztása mindig az adott szervezet, valamint a projekt adottságai alapján történik, sőt lehetőség van a két megközelítés kombinációjának az alkalmazására is. A továbbiakban ezt mutatjuk be.

Az elsődleges vagyonelemek (adatok, alkalmazások) meghatározására a folyamat alapú megközelítést javasoljuk, amennyiben ehhez a megfelelő peremfeltételek rendelkezésre állnak. A szervezet folyamat alapú működése azt jelenti, hogy minden tevékenység folyamatszinten formalizált, az egyes folyamatok leírása utasításként jelenik meg, az egyes folyamatokat nyilvántartják, rendszeresen felülvizsgálják, szükség esetén átdolgozzák és frissítik. Minden egyes folyamat rendelkezik felelőssel (folyamatgazdával). A szervezet üzleti folyamatainak kialakítása és nyilvántartása érdekében általában üzletifolyamat-tervező eszközt alkalmaz. Lehetséges források így az utasítások, azok nyilvántartása, és az üzletifolyamat-tervező eszköz. A cél, hogy az elsődleges vagyonelemek minél nagyobb mértékben automatizált módon azonosításra kerüljenek – ezért célszerű a folyamattervező eszköz használata, mint elsődleges adatforrás. Problé-

ma adódik abból, ha nem azonos minőségű (kidolgozottságú) folyamatok szerepelnek a folyamattervezőben, illetve ha nem egységes névterminológiát használnak a folyamatok dokumentálásakor (pl. azonos adatkört más névvel azonosítanak eltérő folyamatokban). Ilyen esetben lehetőség van az adatok utasításokból történő pontosítására, azonban ez jelentős erőforrás- és időszükséglettel járhat. Az eltérések egyik oka lehet például, hogy az egyes folyamatokat nem ugyanazok a személyek tervezik, hanem az adott folyamatok működését jól ismerők, az adott szakterület szakemberei tervezik meg.

Az elsődleges vagyonelemek folyamat alapú azonosítása sok tanulsággal szolgálhat magának a folyamat alapú működésnek, a folyamatok kidolgozásának és naprakészségének minőségét illetően. Úgy gondoljuk, a tapasztalatok összefoglalása és a visszajelzés fontos e tekintetben is. Ugyanakkor véleményünk szerint a folyamatok kidolgozása és dokumentálása kapcsán felmerülő tényleges hibák és hiányosságok javítása nem lehet a kockázatkezelési projekt feladata és hatékonyan nem is végezhető el egy ilyen projekt keretein belül.

3.2.2.1. Bizalmasság (B)/Sértetlenség (S)/Rendelkezésre állás (R) értékek meghatározása

A vhr alapján a B/S/R értékeket ötfokozatú skálán kell meghatározni, valamint „a veszélyeztetettségnek a bekövetkezés valószínűségének megfelelő kárértékszinteknek megfelelő biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelménye külön-külön értékelendő.”

Az elsődleges információs vagyonelemek B/S/R értékeinek meghatározásában kompetenciával elsődlegesen a folyamat üzemeltetője, az adott üzleti terület rendelkezik. Az egyes folyamatok elvárt R értékeit a szervezet üzletmenet-folytonossági terve (ÜFT) rögzíti. Joggal feltételezhető, hogy kritikus infrastruktúra elemeket üzemeltető szervezetek esetében ez rendelkezésre áll. Így a folyamatokban részt vevő információs vagyonelemekre az R érték örökíthető. Fontos azonban, hogy a folyamatot nem minden esetben akasztja meg egy-egy vagyonelem elérhetetlensége. Tehát R értékének örökítésével erőforrás takarítható meg, ugyanakkor hiba és pontatlanság is keletkezhet. Mérlegelni kell, hogy ez a pontatlanság kezelhető, vagy az adatok pontosítására van szükség. A B és S értékek meghatározására többféle interjúzási technika áll rendelkezésre:

- online adatgyűjtés (e-mail, elektronikus felület),
- személyes megkérdezés (interjú, workshop).

Az e-mailes megkeresés alacsonyabb erőforrás-szükséglettel rendelkezik, ugyanakkor nem egységes, pontatlanabb eredményeket produkál, hiszen a meghatározásokat az egyes kitöltők más és más módon értelmezhetik.

Az interjúk alkalmazása lényegesen több erőforrást igényel, hiszen a folyamatgazdákkal interjúidőpontok egyeztetése, esetleges módosítása szükséges. Ugyanakkor a begyűjtött információk minősége miatt jóval egységesebb és pontosabb képet nyújt a valós helyzetről.

Lehetőség van kombinált megoldások alkalmazására: a pontos adatfelvétel érdekében a személyes interjúk készítését választjuk, ugyanakkor az eredményesség fokozása (és nem mellékesen időszükségletének csökkentése) érdekében e-mailben ebben az esetben is (előzetesen) kiküldés-re kerülhetnek az előzetesen azonosított folyamatok, és kapcsolódó információs vagyonelemek.

3.2.2.2. B/S/R értékek konszolidációja

Az adatfelvétel során meghatározott B/S/R értékek további feldolgozása szükséges, hiszen van olyan információs vagyonelem, mely több folyamatban is részt vesz, azonban az egyes folyamatokban más B/S/R elvárások érvényesülnek vele szemben. Így minden olyan információs vagyonelem esetében, mely több folyamatban is részt vesz, az egyes folyamatokból képzett értéket kell a vagyonelemre érvényesíteni.

3.2.3. Támogató vagyonelemek meghatározása

Az elsődleges vagyonelemek nem létezhetnek önmagukban, szükség van valamilyen eszközre azok feldolgozásához. Egy adatbázisban szereplő adat sincs meg az adatbázis-kezelő rendszer, szerver, tárolórendszer nélkül. Eléréséhez szükség van munkaállomásra, hálózati infrastruktúrára stb. Az egyes támogató vagyonelemek azonosításához forrásként célszerű a minden szervezetnél létező tárgyeszköz-nyilvántartást választani kiindulásként. Ez egy bottom-up elvű megközelítést ad, mely a feldolgozás során finomítható. A tárgyi eszközök nyilvántartásában minden egyes eszköz megtalálható, és mindegyikhez rögzítve van az is, hogy az adott eszköz kinek a használatában van.

A nyilvántartás adatai, valamint a korábban már összeállított folyamatadatok alapján elkészíthető a támogató információs vagyonelemek listája, valamint a B/S/R értékek meghatározása. A szerverek, tárolórendszerek és egyéb, a gépteremben elhelyezkedő számítástechnikai eszközök (központi infrastruktúra) az összes folyamatot figyelembe véve célszerűen a legmagasabb előforduló besorolást kapják, aminek elsődleges oka, hogy a szervezetek jelentős része ma már szinte kizárólag virtualizált környezetet alkalmaz, így nem rendelhetők egyértelműen az egyes eszközök egy-egy informatikai alkalmazáshoz. Ez a tény az Ibtv. által használt rendszerértelmezés alkalmazása során problémákat vethet fel.

3.2.4. Kockázatok azonosítása

A kockázatok azonosítása a következők szerint történik:

- El kell készíteni vagy frissíteni kell a fenyegetés és veszély katalógust, mely alapját képezi a következő lépéseknek. A katalógust ajánlott az Ibtv. szakmai tartalmának megfelelően összeállítani;
- Fel kell mérni a jelenleg érvényben lévő biztonsági intézkedéseket és azok hatókörét;
- vagyonelemként fel kell mérni a következő jellemzőket: a vagyonelem vonatkozásában releváns fenyegetések, veszélyek, a bekövetkezési valószínűségek, valamint a meglévő intézkedések.

3.2.5. Kockázatok számszerűsítése

A B/S/R értékek, valamint a sebezhetőségek, veszélyek, bekövetkezési valószínűségek alapján számszerűsítésre kerülnek az egyes kockázatok. A meghatározott kockázatok mértékét csök-

kentik a már meglévő intézkedések, így ezeket is figyelembe kell venni a számszerűsítés során. A kockázatok „forintosításához” a már meghatározott biztonsági osztályok is irányt mutatnak.

3.2.6. Kockázatok kezelése

A kockázatok mértékének meghatározására több módszer is kidolgozásra került.¹⁶ Mi a kockázatok kezeléséről szóló döntés meghozatalához a széles körben elterjedt CCTA Risk Analysis and Management Method (CRAMM) alkalmazását javasoljuk. Egy CRAMM mátrixa látható az 1. ábrán.

Figyelembe véve a jogszabályi hátteret, az 5 × 5-ös mátrix alkalmazása a célszerű. A zöld mezőbe került kockázatok esetében nem kerülnek kidolgozásra új kockázatjavító intézkedések, azok elfogadásra kerülnek. A sárga tartományba került kockázatok esetében a szervezeti működésnek megfelelő döntés szükséges azok további kezeléséről, míg a piros tartományba került kockázatok kezelésére intézkedési terv kidolgozása szükséges.

1. ábra • Példa a CRAMM mátrixra (saját szerkesztés)

		Üzleti hatás				
		I	II	III	IV	V
Gyakoriság	1	Elfogadható	Elfogadható	Elfogadható	Elfogadható	Döntés
	2	Elfogadható	Elfogadható	Elfogadható	Döntés	Kezelendő
	3	Elfogadható	Elfogadható	Döntés	Kezelendő	Kezelendő
	4	Elfogadható	Döntés	Kezelendő	Kezelendő	Kezelendő
	5	Döntés	Kezelendő	Kezelendő	Kezelendő	Kezelendő

3.2.7. Intézkedési terv kidolgozása és végrehajtása

Minden kezelendő és kezelésre kiválasztott kockázat esetében intézkedési terv kidolgozása szükséges. Az intézkedési terv kidolgozásánál elsődleges szempont a költséghatékonyság, valamint hogy a terv végrehajtásához szükséges erőforrások rendelkezésre álljanak. Figyelembe kell venni a környezetet, valamint az adottságokat. Érdemes előnyben részesíteni azon intézkedéseket, melyek több kockázat mértékét is csökkentik. Az intézkedési tervben foglaltak végrehajtásának ellenőrzésére rendszeres felülvizsgálatot kell végezni. Eltérések, nem megfelelő eredmény esetén beavatkozás szükséges, melyet akár a környezet változása is okozhat. A 2. ábrán látható az ismertetett kockázatelemzési folyamat grafikusán ábrázolva.

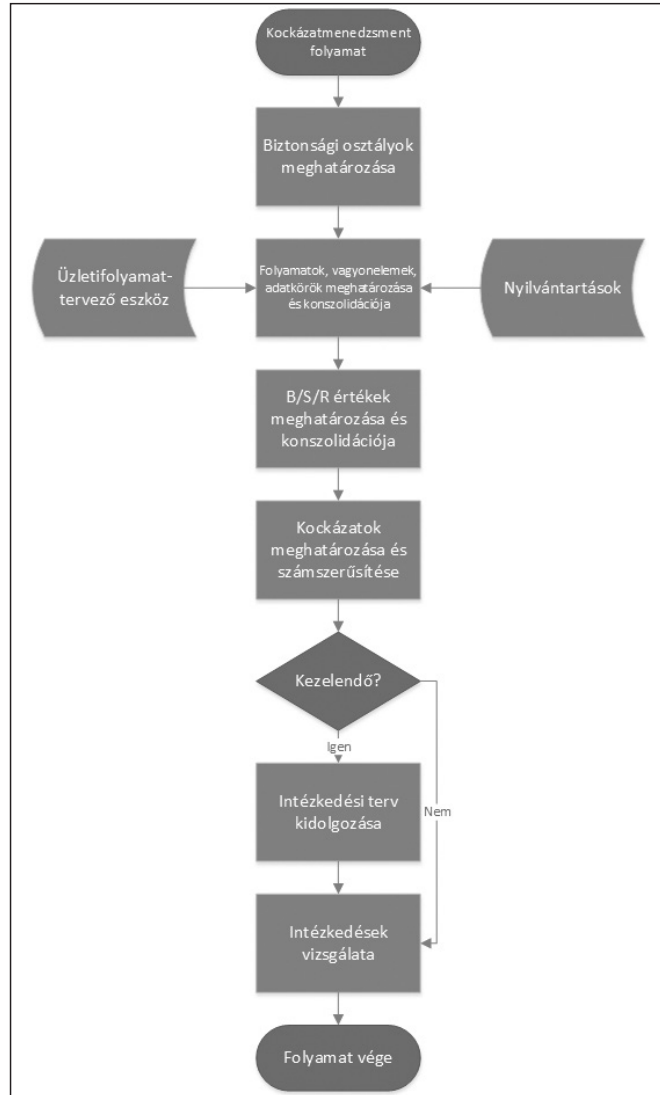
4. KONKLÚZIÓ

Az informatikai rendszerek térhódításával együtt jár a kockázatok számának, a rendszerek sérüléséből eredő károk mértékének ugrásszerű növekedése. Ma már egyetlen szervezet mű-

16 MÓGOR Tamásné, RAJNAI Zoltán: *Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása*, Bolyai Szemle, 33(2014)/2, 43–59.

ködéséből sem hiányozhat az információbiztonsági tevékenység. Különösen igaz ez a kritikus infrastruktúra rendszereket üzemeltető szervezetek esetében, ahol törvényi szabályozás rögzíti az információbiztonsági tevékenység kereteit és elvárásait.

2. ábra • Kockázatelemzési folyamat grafikusán ábrázolva (saját szerkesztés)



Ennek tükrében mutattuk be az információbiztonsági kockázatkezelési tevékenység folyamatának egy olyan lehetséges kialakítását, amely egyszerre veszi figyelembe a vonatkozó szabvány (mint legjobb gyakorlat) elvárásait és a jogszabályi követelményeket. A két követelményrendszer harmonizálható, a szervezet adottságait is figyelembe vevő működési keret alakítha-

tó ki. Ebben a keretben a konkrét lépések megfelelő kiválasztásával felépíthető egy hatékony és eredményes kockázatkezelési tevékenység. Erre egyrészt példákat mutattunk, másrészt alternatívák is választhatók. A kialakított folyamatot nem hisszük sem egyedül üdvözítőnek, sem véglegesnek – a gyakorlati tapasztalatok magukkal hozzák a továbblépés lehetőségét.

• • • • •

SUMMARY IN ENGLISH: Operating critical infrastructures requires integrated IT systems; however, their widespread use inevitably involves the increase in the number of risks and potential damages resulting from system vulnerabilities. An effective IT security strategy is fundamental for any organization; especially in case of critical infrastructure systems, whose IT security framework and requirements are laid down by national legislation. In this paper we describe a possible solution for IT security risk management, utilizing our professional experience, which simultaneously meets the demand of different standards and related laws and regulations. According to our results it is possible to conciliate both requirements and develop a highly effective security framework suitable for several organizations increasing their security level.

Répás Sándor (RSandor@ahol.co.hu): gazdálkodás és menedzsment alapképzési szakon diplomázott 2009-ben a Budapesti Corvinus Egyetemen, majd 2011-ben villamosmérnöki alapképzési szakon, az Óbudai Egyetemen. Okleveles villamosmérnöki képzettséget 2013-ban a Széchenyi István Egyetemen szerzett. 2013-ban elnyerte a Nemzeti Kiválóság Program ösztöndíját. 2002 óta foglalkozik az informatika mellett informatikai és információbiztonsági képzésekkel is. 2004-től kezdődően munkájában az informatikai biztonság került előtérbe. 2014-től kezdődően független hálózati és hálózatbiztonsági tanácsadóként dolgozik. Munkái során részt vett hálózatok tervezésében, kivitelezésében, információbiztonsági ellenőrzésekben, auditfelkészítésekben, kapcsolódó szabályzatok kidolgozásában, etikus behatolási tesztek elvégzésében. Jelenleg PhD-hallgató. Kutatási területe az IPv6 bevezetése, valamint a kritikus információs infrastruktúrák biztonsága. Fontosabb gyártói minősítései: CCSI, MCT, CISA, CISM, CRISC, MTCC. Jelentősebb szakmai szervezeti tagságai: IEEE, ACM, HTE, ISACA, MEE, MKT, NJSZT.

Dr. Dalicsek István (dalicsek.istvan@scetix.hu): a Budapesti Műszaki Egyetem villamosmérnöki karán szerzett okleveles villamosmérnöki diplomát 1982-ben, majd ugyanitt egyetemi doktori fokozatot ért el 1987-ben (BME 4697/1987). A Budapesti Közgazdaságtudományi Egyetem Vezetőképző Intézetének London Business School programjában kapott MBA szakoklevelet 1997-ben. Többéves, hazai nagyvállalatoknál és nemzetközi tanácsadó cégeknél szerzett vezetői tapasztalatok birtokában 2005-ben alapította meg saját vezetői tanácsadóval foglalkozó vállalkozását, melynek azóta is szakmai és adminisztratív irányítója. A cég egyik kiemelt tevékenységi területe az informatikai és információbiztonsági tanácsadás. Az integrált biztonságirányítási rendszerek működtetése és az információbiztonsági kockázatok kezelése területén több sikeres projektreferenciával rendelkeznek mind a vállalati, mind az államigazgatási szektorban.

A FELHASZNÁLÓI PROFIL SZEREPE AZ INFORMÁCIÓBIZTONSÁGBAN

Az információbiztonság kialakítását jogszabályok írják elő az állami és önkormányzati szervezetek számára, amelyek komplex szabályozási környezet kialakítását és információvédelmi megoldások bevezetését szorgalmazzák. Az előírások nagy hangsúlyt fektetnek a feladatok elvégzéséhez szükséges és elégséges minimális jogosultság elvének megvalósítására, a felhasználókat saját feladataik elvégzésére korlátozó kontrollrendszer kialakítására. Emellett a kulcsfontosságú vagy nagy mennyiségű személyes adatot kezelő szervezetek számára kötelezővé teszi az informatikai rendszerek naplóbejegyzéseinek elemzését. Figyelembe véve, hogy a leggyengébb láncszem az ember, a naplóelemzés egyik legfontosabb eleme a felhasználói tevékenységek elemzése, felhasználói profil kialakítása, ezek alapján a szokatlan tevékenységek azonosítása és elemzése a munkatársakról rendelkezésre álló adatok alapján. A tanulmány a felhasználói profil kialakításának és elemzésének célját, lehetőségét, fontosságát, megvalósítási lehetőségeit és korlátait tárgyalja, a hatékonyság, teljeskörűség, valósidejűség, hamis riasztások és adminisztrációs feladatok minimalizálásának tükrében, a felhasználókról elektronikus formában rendelkezésre álló adatok mentén. Ezt követően egy költséghatékony elméleti modellt mutat be felhasználói tevékenységek automatizált elemzésére és annak alapján felhasználói profil kialakítására.

KULCSSZAVAK:

felhasználói aktivitás, jogosultság, konfigurációkezelés, SIEM rendszerek, személyazonosság, szerepkör



1. BEVEZETÉS

Számos, tanácsadó cégek által készített nemzetközi felmérés igazolja, hogy a legnagyobb információbiztonsági kockázatot az információs rendszereket alkalmazó és üzemeltető ember,

munkavállaló, ill. vezető jelenti.^{1,2,3} A humán kockázatot – amely fokozottan jelenik meg a közigazgatásban (személyes adatok, szolgálati és államtikok védelme) – az információtechnológia fejlődése is fokozza. Gondoljunk csak a közösségi oldalakra, a saját mobileszközök munkahelyi alkalmazására.

Fontos kérdésként jelenik meg az állami és önkormányzati intézmények esetében a humán kockázatok csökkentése (az információbiztonság megerősítésének érdekében), az alkalmazható eszközök azonosítása és hatékonyságának vizsgálata. Jelen tanulmány arra keresi a választ, hogy a felhasználóprofil-elemzés milyen módon és feltételek mellett, milyen hatékonysággal járulhat hozzá az intézmények információbiztonságához.

Az emberi tényező kockázatkezelésének egyik módja lehet a hagyományos személyazonosság-, jogosultság- és szerepkörkezelés szabályozása, valamint új eszközökkel történő kiegészítése. A fájlservereken rendszeresen lekérdezhető a bizalmas állami, ill. intézményi dokumentumokhoz és adatokhoz történő hozzáférések (File Audit). Természetesen ennek feltétele az adatok, adatfájlok bizalmasság szerinti osztályozása is.

Felhasználói profil készítésével az információs rendszerek működése, üzemeltetése során folyamatos „megfigyelést” végezhetünk. A megszokottól eltérő viselkedés esetén megvizsgálható a felhasználó motivációja, információbiztonsággal kapcsolatos ismeretei, hozzáállása és tudatossága. Ez egy preventív információvédelmi tevékenységet jelent, ami nem tekinthető az információvédelmi vezető paranoiájának. A rutinszerű és szabályos működést rögzítő adatbázisokból kiszűrhetők azok a naplózási adatok, amelyek a felhasználói viselkedés szokatlanságát mutatják.

A korszerű SIEM (Security Information and Event Management) rendszerek segítségével átfogó képet kaphatunk a szervezet információbiztonsági tevékenységéről.⁴ Az ilyen speciális informatikai alkalmazás rögzíti és gyűjti a biztonsággal kapcsolatos eseményeket a végfelhasználó, az adatforgalom, a hálózat és a biztonsági eszközök (pl. tűzfalak, vírusirtók, behatolásjelzők) vonatkozásában. Az események biztonsági vizsgálata a „szokásos” működéshez történő viszonyítást jelenti. A különböző forrásokból származó naplóadatok összefuttatása és elemzése révén könnyen behatárolhatjuk a szándékos vagy a véletlen károkozást.

1 ERNST & YOUNG: *Get ahead of cybercrime EY' Global Information Security Survey*, 2014, 40. Forrás: [www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/\\$FILE/EY-global-information-security-survey-2014.pdf](http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf) (2015. 02. 27.)

2 PwC: *Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security*, 2015, 40. Forrás: www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml# (2015. 02. 27.)

3 A FROST & SULLIVAN Market Study in Partnership with ISC2: *The 2013 (ISC)² Global Information Security Workforce Study*, 2013, 28. Forrás: www.isc2cares.org/uploadedFiles/wwwisc2cares.org/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf (2015. 02. 27.)

4 David R. MILLER, Shon HARRIS, Allen HARPER, Stephen VANDYKE, Chris BLASK: *Security Information and Even Management (SIEM) Implementation*, McGraw–Hill, 2014, 464.

2. PARADIGMAVÁLTÁS AZ INFORMÁCIÓ- ÉS IT-BIZTONSÁGI KOCKÁZATOK ELEMZÉSÉBEN

A szervezetek ez idáig a felhasználókat korlátozó, az üzleti folyamatokat kiszolgáló információs rendszereket pedig szigorúan szabályozó, kontroll alapú biztonsági megközelítést alkalmazták. Ez a teljes körű „védekezés” (esemény-ellenőrzés a nap 24 órájában, különböző egymást átfedő biztonsági technológiák kezelése, naplóelemzés, üzemeltetés) amellet, hogy megterhelje az informatikai személyzetet, a változó fenyegetések miatt egyre kevésbé tekinthető hatékonynak.

Az informatikai biztonsági szolgáltatások mára már sok tehermentesítő lehetőséget biztosítanak:⁵

- tűzfalmenedzselés,
- automatikus napló- és logelemzés (adathozzáférések monitorozása),
- belső sérülékenységi vizsgálata (hálózaton belüli eszközök felderítése, osztályozása, elemzése, kockázatértékelés, sérülékenységek javítása és azok ellenőrzése),
- internetes alkalmazások automatikus biztonsági ellenőrzése,
- wifibiztonság ellenőrzése,
- hálózati hozzáférés ellenőrzése (felhasználói hitelesítés, nem megfelelő felhasználók kezelése, illetéktelen hozzáférési végpontok kizárása),
- behatolásjelzés,
- érzékeny adatok adatosztályozás utáni kiemelt kezelése,
- és végül, de nem utolsósorban az eseménymenedzselés (infrastruktúra, az eszközök és alkalmazások naplóelemzése).

A SIEM rendszerek alkalmazása a felhasználók viselkedésének folyamatos megfigyelését és a szokatlan tevékenységek matematikai módszerekkel (eloszlásvizsgálat, minták keresése, szöveganalízis) történő kiszűrését, valamint célorientált kivizsgálását jelenti. A naplóüzemek kockázatok szerinti rangsorolása után történik a személyzet riasztása, akik így csak az igazán fontos és kockázatos eseményekre koncentrálhatnak. A biztonsági intézkedések eredményességét növelheti a kockázatelemzés területének észszerű szűkítése.

A naplózás során rögzítésre kerül, hogy mi és mikor változott, ki volt a végrehajtó és milyen hozzáférési pontról indították az aktuális tranzakciót, valamint az is, hogy a változtatás engedélyezett/jóváhagyott volt-e.

Az információs rendszerek biztonságát és ehhez kapcsolódóan a szervezet információbiztonságát több oldalról is vizsgálni szükséges. A SIEM rendszerek hatékonysága megkívánja az illesztést a szervezeti információbiztonsági intézkedésekhez (politikához), IT-eszközökhez és a szervezeti folyamatokhoz.

5 PÓSER Valéria, SCHUBERT Tamás, KOZLOVSZKY Miklós, PRÉM Dániel: *Security on-demand megoldások az informatikai infrastruktúrákban*, Hadmérnök, 8(2013)/3, 211–222.

Az információvédelemben több biztonsági szintet is megkülönböztetünk:⁶

- információtechnológiai infrastruktúra (konfigurációkezelés, hardver-, szoftver- és hálózatzvédelem);
- információkezelés (adatfelvétel, -módosítás, -törlés, informálódás, ill. lekérdezés);
- ügyviteli folyamatok (folyamatszabályozás, workflow, termékek és szolgáltatások informatikai támogatása, vevőszolgálati tevékenység);
- szervezet (információbiztonsági stratégia, kockázatkezelés, szervezeti struktúra, vezetési stílus, szervezeti kultúra, vezetői feladatok támogatása).

Erre jó példa a jogosultsági rendszer „holisztikus” kialakítása. Mind a négy szinten vannak ezzel kapcsolatos feladatok:

- IT-szint – felhasználóazonosítás,
- információkezelési szint – csak a munka elvégzéséhez minimálisan szükséges adathozzáférések biztosítása,
- folyamatszint – kritikus folyamatok megosztása, helyhez és személyhez kötött jogosultság,
- szervezeti szint – kockázatkerülés, jogosultsági csoportok kialakítása és a jogosultsági rendszer állandó felügyeletének szabályozása.

Maria Karyda és szerzőtársai⁷ olyan általános információs rendszerekre alkalmazható biztonsági működési modellt dolgoztak ki, amelyben a biztonsági szintek mellett szerepet kap:

- a változáskezelés (szervezeti felépítésben, szervezeti magatartásban, folyamatokban és az információtechnológiában) – mint *információtartalom*,
- a külső és belső kapcsolatok, *összefüggések* (gazdasági, jogi, politikai és szociális tényezők, iparági verseny, beszállítói viszonyok, szervezeti kultúra belső elemei),
- valamint az üzleti folyamatok kulturális és hatalmi szempontból történő megközelítése (biztonsági igények megjelenése a szervezeti kultúrában és a hatalmi viszonyok érvényesítése az információbiztonsági politikában).

3. JOGOSULTSÁG-, SZEREPKÖR- ÉS SZEMÉLYAZONOSSÁG-KEZELÉS

A tranzakciófeldolgozó és vezetői információs rendszerek támogatják, modellezik és sok esetben optimalizálják a szervezet értékteremtő és kiszolgáló folyamatainak végrehajtását. A munkatársak (a felhasználók) az információtechnológiai erőforrásokhoz hozzáférve munkakörükből adódó „elemi” feladatokat látnak el. Adatokat rögzítenek, módosítanak, lekérdeznek, esetleg törölnek azért, hogy az információ – mint erőforrás – biztosítva legyen a különböző szintű döntéshozóknak.

Sok felhasználó és több, inhomogén információtechnológiai alapokon nyugvó információs rendszer esetén a felhasználók azonosítása és rendszereléréseik nyomon követése teljesen kaotikussá válhat. Rések és/vagy átfedések keletkezhetnek a hozzáféréseknél. A jogosultsá-

6 Ji-Yeu PARK, Rosslin John ROBLES, Chang-Hwa HONG, Sang-Soo YEO, Tai-Hoon KIM: *IT Security Strategies for SME's*, International Journal of Software Engineering and its Applications, Vol. 2. No. 3., July 2008, 91–98.

7 Maria KARYDA, Evangelos KIOUNTOUZIS, Spyros KOKALAKIS: *Information systems security policies: a contextual perspective*, Computers & Security 25., 2005, 246–260.

got nem mindig a tényleges feladat- vagy munkakör alapján határozzák meg. Inkább informális szokásokat és hagyományokat vesznek figyelembe. Többszörös felhasználókezelés alkalmazhat ki az egymástól független információs rendszerekben. Változások alkalmával (át helyezés, kilépés, új folyamatok, kiszervezés stb.) ad hoc módon végzik a jogosultsági kérdések – sok esetben utólagos – adminisztrációját.

A megoldás a folyamatok és szervezet elemzésén alapuló szerepkörök kialakítása lehet, ami azután összekapcsolódhat a szerepekbe bekerülő felhasználók személyazonosságának kezelésével.

A felhasználó a folyamatok végrehajtásából adódó feladatainak elvégzéséhez információtechnológiai eszközöket is alkalmaz. Természetesen nincs szüksége minden IT-erőforrásra és minden tárolt adatra. A *jogosultság* korlátozza a felhasználó közreműködését, optimális esetben csak a munkaköréből adódó tényleges információkezelési feladatok elvégzését teszi lehetővé, de azt viszont teljeskörűen. Meghatározásának alapja a folyamat(ok), azok céljai, a szervezeti felépítés és az informatikai infrastruktúra. Szerepet játszanak benne az információbiztonsági kockázatok is (értékes állami, ill. intézményi információk elvesztése v. illetéktelen kezekbe kerülése). A tényleges jogosultsági rendszer kialakítására hatással van a szervezeti és egyéni tudás, a szervezeti kultúra, valamint a munkakörhöz rendelt felelősség.

A jogosultság formálisan is nyilvántartható és nyilvántartandó (kiadható, beállítható, ellenőrizhető, jóváhagyható, elutasítható, szüneteltethető, elvehető). Fontos a munkahelyi vezető és az adott terület adatbiztonságáért felelős hozzájárulása. A felhasználó egyszerűbb esetben felhasználói nevet (login) és jelszót (password) kap. Ez magasabb biztonsági igények esetén kiegészíthető vagy helyettesíthető biometrikus „azonosítókkal” vagy kiegészítő hardvereszközökkel. Ezeket rendeljük a folyamatoknak és a szervezeti céloknak megfelelően az információs rendszerek, alkalmazások moduljaihoz, menüihez, menüpontjaihoz, képernyőkhöz és adatmezőkhöz, valamint adatbázis-lekérdezési lehetőségeihez. A jogosultság a felhasználókon túl köthető alkalmazási helyhez és időszakhoz is.

A felhasználónak munkafeladataiból adódóan esetenként akár több szervezetenél működő információs rendszerhez is hozzá kell férnie. Ez azt jelenti, hogy akár többszörösen is „bizonyítani” kell jogosultságát. Ez történhet a felhasználó birtokában lévő (You have...) azonosításra alkalmas eszközökkel (chip- és mágneskártyák, hardverkulcsok).

A tudásalapú (You know...) azonosítás sok rendszer esetén már nehezen megvalósítható. Hiszen egy magánembernek is mennyi jelszót és/vagy PIN kódot kell fejben tartania. Ráadásul ezeket biztonsági okokból időközönként illik megváltoztatni. Segítségét és egyszerűsítést jelenthet, ha biometrikus elemeket (ujj- és tenyérnyomat, írisz, véna, DNS) is használunk azonosításra (You are...), de ezek használata személyiségi jogi kérdéseket is felvet. A munkáltató (intézmény, államigazgatási szerv) nem kérheti minden esetben ezek alkalmazását a munkavállalójától. Az azonosítás egyébként is a védelmi tevékenység felhasználót érintő része.

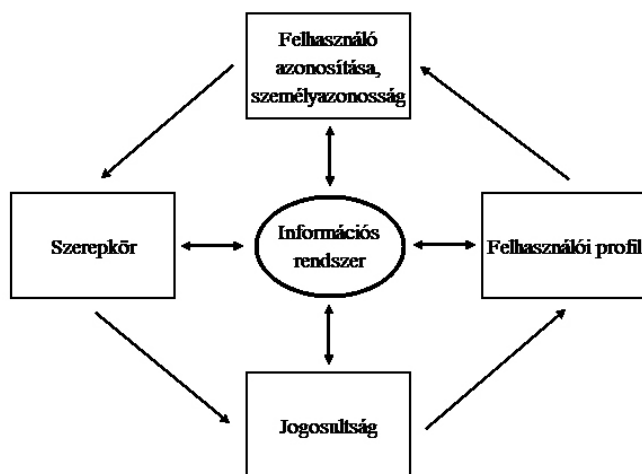
A biztonság a megfelelő *szerepkör* és a hozzá kapcsolódó jogosultsági rendszerek révén válna teljessé. Nagyobb létszámú, több telephelyes „szabványosított” folyamatokat végrehajtó szervezetek esetén megfontolandó szerepkörök kialakítása. Ugyanabban a szerepkörben dolgozó felhasználók azonos jogosultságot kapnak. A szerepkör nem csak egy informatikai alkalmazáshoz köthető. Így a jogosultságok beállítása automatizálható és nagy számban

egyszerre változtatható. A felesleges hozzáférések kiszűrhetők, és az egyéni jogosultságok száma csökkenthető. A szerepkörök száma tehát kevesebb lesz, mint a felhasználók száma.

A szerepkörök köthetők folyamatokhoz (folyamatelemekhez) és szervezeti egységekhez. Az előbbi a szervezet tevékenységének funkcionális kiszolgálását teszi lehetővé, az utóbbi pedig a szervezeti működést és a döntéshozatalt támogatja. A szerepkörök „állandóak”, az információtechnológia fejlődése vagy új folyamatok változtathatják csak meg. A felhasználói fluktuáció így kevésbé van hatással az intézményi, ill. állami információs rendszerek működésére. A legtöbb IT-kereskedelemben kapható, tranzakciókezelésen alapuló megoldás már használja az ún. szerepkör alapú hozzáférés-ellenőrzést (Role Based Acces Control). A szerepkörök kialakításának kezdetén a tényleges folyamatokon és szervezeten alapuló szerepelvárás általában nem egyezik meg az informatikai megoldások által biztosított információkezelési lehetőségekkel. A szerepkör-kialakítás egyik fontos célja tehát az információtechnológia és szervezeti működés összhangba hozása.⁸

A *személyazonosság-kezelés* révén azonosíthatjuk a munkatársakat és a külső partnereket egy vagy több szervezethez tartozó információs rendszerben. Így szabályozhatjuk hozzáférésüket a különböző információtechnológiai erőforrásokhoz. Összeköti a felhasználói jogosultságokat és tiltásokat a rendszerekben meglévő információkezelési feladatokkal. Ez akkor válik különösen fontossá, amikor a szervezetnek több, egymással kapcsolatban álló, eltérő információtechnológiai infrastruktúrán alapuló információs és kommunikációs rendszere is van. Nem feladata a felhasználói hozzáférés hitelesítése (authentication) és új jogosultság (authorisation) létrehozása. Végigköveti a felhasználói életciklust egyénenként (pl. belépést, munkakör-bővülést, átszervezésből adódó pozícióváltást, hosszabb fizetés nélküli szabadságot vagy a kilépést) (1. ábra).

1. ábra • A felhasználóanalízis részterületei (saját szerkesztés)



8 Heiko KLARL, Korbinian MOLITORISZ, Christian EMIG, Karsten KLINGER, Sebastian ABECK: *Extending Role-based Access Control for Business Usage*, SECURWARE '09, The Third International Conference on Emerging Security Information Systems and Technologies, Athens/Glyfada, Greece, June 18–23., 2009, 136–141.

Az információs rendszereket üzemeltető szervezetek a *felhasználói profil* megalkotásával, folyamatos karbantartásával és a szokatlan viselkedés kiszűrésével a végtelen károkozás lehetőségeire is felhívhatják a munkavállaló figyelmét.

A felhasználói profil kialakítása során felhasználjuk a naplókat, amelyekben rögzítésre kerülnek a felhasználó által kezdeményezett adatmozgások (információkérés, új adat rögzítése, adat módosítása vagy törlése) és tranzakciók.

A felhasználói viselkedés alapján kapott adatok gyors elemzésével és a szokatlan viselkedési formák kiszűrésével kezelhetők a felhasználók információbiztonsági kockázatai. A szokatlanosság (unusuality) mindenképpen kockázati tényező.

4. A FELHASZNÁLÓK CSOPORTOSÍTÁSA

A felhasználói viselkedés vizsgálatát érdemes felhasználói csoportok kialakítása után elvégezni. J. M. Stanton és szerzőtársai (2005) a felhasználókat két tényező alapján sorolták be:⁹

- IT és IT-biztonsági szakértelem (expertise) – alacsony vagy magas,
- felhasználói szándék vagy hozzáállás (intentions) – rosszindulatú (malicious), semleges (neutral) vagy támogató (beneficial).

Az alkalmazott lehet elégedetlen (akár tudatos szabotőr is), naiv, vagy külső szervezet által felbérlet is. A vizsgálat szempontjából az indíték meghatározása is fontos lehet.

Ez kiegészíthető generációs különbségekből származó, információbiztonságot is érintő szokásokkal is. A szociológusok szerint a mai munkavállalók születési adataik alapján öt csoportba sorolhatók:¹⁰

- veteránok (1946 előtt születtek; munkavállalói szempontból már nem érdekesek),
- „baby boom” generáció (születési idő: 1946–1965),
- X generáció (születési idő: 1965–1980),
- Y generáció (1980 és 1995 között születtek),
- Z generáció (1995 után jöttek a világra).

Az öt generáció eltérő biztonságtudatosságot képvisel, mindegyikre más-más információbiztonsági kockázat jellemző.¹¹

Csoportosítási szempont lehet a szervezeti hierarchiában betöltött szerep is. Érdemes megkülönböztetni a felhasználókat a közép- és felsővezetőktől, valamint az információs rendszerek üzemeltetéséért felelős szakembereket is.

9 Jeffrey M. STANTON, Kathryn R. STAM, Paul MASTRANGELO: *Analysis of end user security behaviors*, Computers & Security, 2005/24, 124–133.

10 Lynne C. LANCASTER, David STILMANN, Harvey MACKAY: *When generations collide*, New York, First Collins Business Edition, 2005, 355.

11 MICHELBERGER Pál, BEINSCHRÓTH József, HORVÁTH Gergely Krisztián: *The Employee, An Information Security Risk = Acta Oeconomica Universitatis Selye*, 2(2013)/1, 187–200.

5. BIZTONSÁGTUDATOSSÁG

A felhasználók a védendő információkhoz munkájukból (és jogosultságukból) adódóan hozzáférnek. Rosszindulatú támadás esetén kézenfekvő, hogy a támadó a felhasználó biztonság tudatosságai hiányosságait próbálja kihasználni.

A profil elemzése során fény derülhet a szokatlan felhasználói viselkedésre, és meghatározható a gondatlanság, esetleg a szándékos károkozás is. Ez alapján a felhasználót tájékoztathatjuk a tevékenységéből adódó kockázatokról, kérhetjük a biztonsági szabályozás betartását, valamint javíthatunk a nem megfelelő munkakörnyezeten is.

A tudatosságot, ill. az információbiztonságot gyengítheti az új eszközök, szoftverek kellő biztonsági ismeret nélküli szervezeti alkalmazása (pl. fájlmegeosztók, hordozható eszközök, közösségi oldalak).

A felhasználók gyakran érzik azt, hogy az információbiztonsági szabályozás nem egyértelmű, nehezen betartható, és nem illeszkedik a szervezeti folyamatokhoz.¹² Nincs összehangolva a szerepök és a felelősség. Ilyenkor „találják ki”, hogy hogyan használják az információs rendszereket. Tudatos felhasználóként nyilatkoznak felméréseken és vizsgákon, de egy-egy egyedi esemény kezelésekor a praktikus és gyors üzleti eredményt tartják fontosabbnak. A helyzet-tudatosság (situation awareness),¹³ ill. annak hiánya nagyban befolyásolja az információbiztonságot. A felhasználóknak fontos lenne megérteni, hogy a kezelt információ mit jelent számukra most, és mit jelenthet majd a jövőben, milyen célok megvalósításához (lesz) szükséges.

Az eseménymenedzsment révén kontrollálható egy ún. „social engineering” audit is. Ennek során egy független külső szakértői csoport megpróbálja feltérképezni a szervezet információbiztonsági szempontból gyenge pontjait (biztonsági réseket) és tesztelni a kialakított védelmi intézkedéseket. Ez behatolást (fizikai is), információ-hozzáférést, eszköztulajdonítást, kémprogram-telepítést, adathalászatot, fertőzött program/fájl beküldését, ill. ezekre tett kísérletet jelent.

6. A FELHASZNÁLÓ ANALÍZISE

A felhasználó tulajdonságainak, szokásainak és viselkedésmódjának elemzése annak munkavégzése során, ami a felhasználói profiljával elvégzett feladatok végrehajtásának és végrehajtási módjának vizsgálatával történik. A vizsgálat során felhasználhatók a munkáltató felhasználóról nyilvántartott adatai, és munkavégzése során az információs rendszerekben elvégzett feladatainak naplóbejegyzései. Az így előállított adatok alapadatként használhatók fel az információbiztonsági naplóelemzés során, szokatlan események azonosításának és információbiztonsági események kiszűrésének érdekében. A naplóelemzések új információkat szolgáltathatnak a felhasználói profilról, amelyek visszacsatolhatók annak pontosításához.

12 Eirik ALBRECHTSEN: *A Qualitative study of users' view on information security*, Computers & Security, 2007/26, 276–289.

13 Jeb WEBB, Atif AHMAD, Sean B. MAYNARD, Greme SHANKS: *A situation awareness model for information security risk management*, Computers & Security, 2014/44, 1–15.

7. A FELHASZNÁLÓI AKTIVITÁS ANALÍZISE

A felhasználói aktivitás elemzése az egy felhasználóra jutó információmennyiséget, annak összegyűjtéséhez és elemzéséhez szükséges erőforrásokat figyelembe véve nagyobb szervezetek esetében jelentős feladat, de kisebb szervezetek esetében sem elhanyagolható. A feladatok manuális elvégzése kisebb szervezetek esetében ugyan lehetséges, de a felhasználó személyes és tevékenységére vonatkozó nyers, feldolgozás előtti adatainak hozzáférhetősége visszaélésekre adhat lehetőséget.

A felhasználói profil automatizált elemzéséhez szükség van a felhasználóról rendelkezésre álló adatok lekérésére az elemzést végző SIEM rendszerben. A felhasználókról elérhető információkat rendszerekben tárolható és nem tárolható csoportba sorolhatjuk. A személyes, vagy személyekhez köthető információk tárolása személyiségi jogokat sérthet, és a helyi jogszabályok figyelembevételével kell eljárni a rögzítendő adatok körének meghatározásakor, az adatok rögzítésekor és a felhasználás során is. Ugyanakkor biztosítani kell az adatok biztonságát – bizalmasságát, sértetlenségét és rendelkezésre állását, hogy csak az arra jogosultak férhessenek hozzá, és csak akkor, amikor arra szükség van.

A felhasználói profil összeállításához szükséges ritkán változó, a felhasználó személyes és tulajdonságait leíró adatait tekinthetjük alapadatoknak, amelyek rendelkezésre állnak a szervezet számára:

- a munkaügyi nyilvántartásban, amely tartalmazza:
 - a felhasználó szerepkörét és feladatait;
 - korcsoportját – mely generációhoz tartozik;
 - a szervezetben betöltött pozícióját;
- a beléptető rendszerekben, amelyek szabályozzák, hogy a szervezet telephelyén belül mely területekre van belépési engedélye;
- a munkaidő-nyilvántartó rendszerekben, amelyek szabályozzák, hogy a felhasználó mikor és honnan végezhet munkát,
- az elektronikus címtárban – amely tartalmazza:
 - a felhasználó azonosítóját;
 - az elérhetősége és a munkavégzés helyére vonatkozó információkat;
 - csoporttagságait, amelyek adott esetben hozzáférési jogosultságokat is takarnak;
- a személyazonosság- (Identity Management – IDM) kezelő rendszerekben vagy annak hiányában jogosultság-nyilvántartásban, amelyek támogatják a felhasználóknak kiosztott jogosultságok nyilvántartását;
- a konfigurációkezelési adatbázisban (Configuration Management Database – CMDB), amely tartalmazza a felhasználók által használt eszközöket.

A felhasználói tevékenységek elemzéséhez további adatokra is szükség van, amelyek folyamatosan változhatnak, nem érhetőek el informatikai rendszerekben, de többnyire előállíthatók a felhasználó által elvégzett feladatok naplóbejegyzéseinek elemzése alapján. Ezek lehetnek viselkedési szokások, személyiségi jegyek, segítőkészség, gépelési gyorsaság, felhasználói készség, biztonságtudatosság, szokásos bejelentkezési végpont, bejelentkezési útvonal és

időtartam, informatikai rendszerekben használt parancsok és azok sorrendje. A naplóelemzések során észlelt kisebb eltéréseket érdemes visszacsatolni a rendszerbe a korábban letárolt felhasználói adatok historikus megőrzésével, így az adatok folyamatosan pontosíthatók, a nagyobb eltérések szokatlan eseményeknek minősülhetnek, és további vizsgálat vagy riasztás tárgyát képezhetik.

Információbiztonság szempontjából a felhasználók tevékenységeire vonatkozó adatok képezik a legfontosabb információforrást. Ezt nevezhetjük a felhasználók megfigyelésének is, de valódi célja a szokatlan események azonosítása, kiszűrése és az információbiztonság megerősítésére való felhasználása. Az informatikai rendszerek folyamatosan naplózzák a felhasználók tevékenységeit, hogy bármilyen hiba esetén javítani lehessen az adatokat. Ezek az információk rendszerenként is elemezhetők és értelmezhetők, de információbiztonság szempontjából csak az adott rendszerre vonhatók le következtetések. Mivel az információbiztonság elleni támadások rendszerint több rendszert is érintenek, sokkal hatékonyabban szűrhető ki, ha az összes rendszerben naplózott tevékenység elemzése összevontan történik. A felhasználók tevékenységeinek elemzésében fontos szerepet játszik a biztonsági eszközök naplóbejegyzéseinek, de adott esetben a hálózati adatforgalom elemzése is. Az elemzések SIEM rendszerekben történnek, amelyek összegyűjtik a különböző rendszerekben keletkező naplóbejegyzéseket, komplex algoritmusokkal azonosítják és összeillesztik a tevékenységek összetartozó adatait.

Annak ellenére, hogy mára már léteznek szabványok az események naplózására, a különböző rendszerek sok esetben mégis más-más formátumban hozzák létre a naplóbejegyzéseket. Az eltérések ellenére a naplóbejegyzések legtöbb esetben tartalmazzák az eseményekre vonatkozó lényeges adatokat, amelyek alapján előállíthatók a következő információk:

- ki az esemény kiváltója;
- mi az esemény tárgya – mi történt;
- mikor történt az esemény;
- hol történt az esemény – melyik eszközön;
- melyik objektumon történt az esemény (fájl, adatbázis stb.);
- az esemény forrása – honnan indult az esemény kiváltása;
- mire irányult az esemény.

Ez lehetővé teszi a különböző naplóbejegyzések egységes formátumra hozását,¹⁴ amit normalizálásnak nevezünk, ami alapját képezi az egységes tárolásnak¹⁵ és feldolgozásnak. Vannak olyan informatikai rendszerek, amelyek egy eseményt rendszeres időközönként addig naplóznak, amíg meg nem szűnik annak oka, így a normalizáláson túl fontos szerepet játszik az eseményhez tartozó duplikátumok kiszűrése. Nagyobb szervezeteknél ez nagy mennyiségű adat valós idejű összegyűjtését, feldolgozását és tárolását jelenti. A naplóállomá-

14 SECURISIS: *Understanding and Selecting SIEM/Log Management*, August 25., 2010. 40. Forrás: securisis.com/assets/library/reports/Securisis_Understanding_Selecting_SIEM_LM_FINAL.pdf (2015. 06. 07.)

15 HARGITAI Zsolt: *A belső védelmi rendszer megerősítése* – Információvédelem menedzselése LXIV. Szakmai fórum, Budapest, 2015. január 21., 12–20. Forrás: letoltes.etrend.hu/Hetpecset/ppt_LXIV_3/Novell_Hetpecset_2015.pdf (2015. 03. 16.)

nyok feldolgozásának következő fázisa az események korrelációja, amelynek során a SIEM rendszer bonyolult matematikai modelleket alkalmazva összefüggéseket keres a különböző rendszerekből származó naplóbejegyzések között. Ez egyre fontosabbá vált az APT (Advanced Persistent Threat) támadások megjelenésével, amelyek során a támadó időben elnyújtva, a pillanatot kivárva hosszú időn keresztül hajta végre a támadását, miközben információt gyűjt a szervezetről, annak munkatársairól és eszközeiről.

A felhasználói aktivitás elemzésének megvalósítása komplex feladat. SIEM rendszerek keretében való megvalósítása sok esetben hosszú előkészítést igényel. Rendszerint magas költséggel jár, fenntartásuk folyamatos munkavégzést és költséget generál.¹⁶ Az információbiztonsági piacon megtalálható SIEM termékek különböző funkcionalitást, feldolgozási és riport-előállítási sebességet és időegységre eső naplóbejegyzésdarabszám-elemzési korlátot kínálnak.¹⁷ Egyes termékek az események valós idejű feldolgozásának érdekében naplóbejegyzéseket dobnak el feldolgozatlanul, mások pedig a teljeskörűsége teszik a hangsúlyt, és ezáltal elveszítik a valós idejű reagálási képességet. A legtöbb támadás végrehajtásának átfutási ideje kevesebb, mint 1 óra, de sok esetben percek alatt zajlik le, ezért fontos a valós idejű riasztási képesség. Nagy szervezetek esetében fontos szerepet játszik a skálázhatóság, mivel hatalmas mennyiségű információbiztonsági adat áll elő, amelynek valós idejű elemzése jelentős számítási kapacitást igényel, de a naplóállományok tárolására, utólagos elemzésére és időszakos jelentések elkészítésére is szükség van.¹⁸ Ehhez megfelelő tárolási struktúrákra, tárolási kapacitásra és információvédelmi megoldásokra van szükség.

8. A FELHASZNÁLÓI AKTIVITÁS ELEMZÉSÉNEK AUTOMATIZÁLÁSA

Méretüktől és tevékenységi körüktől függően változnak a szervezetek információfeldolgozási, tárolási és biztonsági szükségletei. A kiépített információfeldolgozási és tárolási kapacitás általában megfelel a szükségletnek, mert elengedhetetlen a napi munkavégzéshez. Mivel az információbiztonság – sok esetben annak sérülése is – láthatatlan, a támogató rendszerek kiépítettsége sok esetben elmarad a szükséges mértéktől, pl. megvalósul a naplóállományok gyűjtése, de nem történik meg azok feldolgozása, elemzése, legfeljebb információbiztonsági incidens kivizsgálásához veszik igénybe.

A rendelkezésre álló naplóállományok feldolgozása felhasználóiaktivitás-elemzéshez és felhasználóiprofil-készítéshez szervezetre szabott SIEM rendszerrel valósítható meg.¹⁹ Mint

16 Jerry SHENK: *Sorting Through the Noise*, SANS Institute Infosec Reading Room, May 2012, 17. Forrás: www.sans.org/reading-room/whitepapers/analyst/eighth-annual-2012-log-event-management-survey-results-sorting-noise-35230 (2015. 08. 01.)

17 J. Michael BUTLER: *Benchmarking Security Information Event Management (SIEM)*, SANS Institute Infosec Reading Room, February 2009, 16. Forrás: www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755 (2015. 07. 05.)

18 Dave SHACKLEFORD: *Security Intelligence in Action: SANS Review of McAfee*, Enterprise Security Manager (ESM) 9.2. SANS Analyst Program, May 2013, 18. Forrás: mpa.co.nz/media/34691/security-intelligence-in-action-sans-review.pdf (2015. 07. 14.)

19 NYIKES Zoltán: *A mobil eszközök biztonsági kérdései, avagy, hogyan használjuk a nyilvános WIFI2 hálózatokat*, Kommunikáció 2014, Nemzeti Közszolgálati Egyetem, Budapest, 2014. november 12., 26.

láthattuk, a felhasználói tevékenység elemzésének automatizálásához számos törzsadat beállítására van szükség, ezek a szervezet fejlettségétől függően állnak rendelkezésre informatikai rendszerekben, ahonnan a SIEM rendszer automatikusan átveheti. Amennyiben az adatok átvétele nem automatizálható, különös figyelemmel kell eljárni annak érdekében, hogy frissítésük megfelelő időben megtörténjen, főleg a felhasználói fiókok és jogosultsági körök létrehozása, módosítása és törlése esetében.

Az első generációs SIEM rendszerek beállítása és karbantartása nehézkes, erőforrásigényes és költséges a hozzáadott értékükhöz képest. A költségek és feladatok csökkentése részben a beállítások automatizálásával, interfészen keresztüli rendszeres beolvasásával és frissítésével, továbbá a naplóállományok elemzésének felhasználásával valószínűsíthető meg. Elindultak kutatások olyan SIEM rendszerek elkészítésére, amelyek minimális konfigurálással és nagy pontossággal szűrik ki a szokatlan eseményeket.

9. A KONFIGURÁCIÓ- ÉS VÁLTOZÁSKEZELÉS SZEREPE A FELHASZNÁLÓI AKTIVITÁS ELEMZÉSÉBEN

A *konfigurációkezelést* értelmezhetjük szűkebb ITIL szerinti értelemben, amely a konfigurációs elemek [informatikai eszközök (hardver, szoftver és hálózat) és felhasználók] és kapcsolataik konfigurációkezelési adatbázisban (CMDB) való nyilvántartásának naprakészen tartásával foglalkozik, „Mi lenne, ha...?” elemzések elvégzésének lehetőségével támogatva a változáskezelést, tágabb értelemben pedig beleértjük a konfigurációs elemek beállításait és azok kezelését is. A konfigurációkezelés szoros kapcsolatban áll az IT-eszközgazdálkodással is, nyilvántartja az eszközök helyét, felelősét, karbantartóit, támogatóit és felhasználóit.

A konfigurációkezelés nagymértékben támaszkodik a *változáskezelésre*, ami fontos szerepet játszik a konfigurációs elemek a CMDB-ben való naprakészen tartásában. A változáskezelés legfontosabb szerepe, hogy nyilvántartsa az IT-változásokérelmeket, nyomon kövesse tervezésüket, kivitelezésüket, megfelelő kontrollt biztosítson a változások biztonságos végrehajtása során és jelezze a konfigurációs elemekben okozott változásokat. A változásokérelmek jóváhagyását és a változások tervezését követően az IT infrastruktúrában okozott módosítások tervezetét érdemes rögzíteni a CMDB-ben, mint az eszközök leendő állapota, a változás végrehajtását követően pedig véglegesíteni azokat.

A konfigurációkezelést támogató megoldásokat is két nagy csoportra oszthatjuk:

- konfigurációs adatbázis automatizált frissítését támogató eszközök, amelyek folyamatosan figyelik az informatikai infrastruktúrát, észlelik a konfigurációs elemekben és beállításaikban történt változásokat, amennyiben azok szerepelnek a változáskezelési nyilvántartásban a tervezett változások között, nyugtázzák, egyébként riasztást küldenek a konfigurációmenedzsernek nem engedélyezett változsról;
- automatizált frissítést nem támogató eszközök, amelyek esetében az adatok frissítése manuálisan történik a tervezett változások kivitelezését követően.

Információbiztonság szempontjából mindkét megoldástípus támogatja a naplóelemzést és ezáltal a felhasználók tevékenységeinek elemzését az eszközök, felhasználók, kapcsolataik és paramétereik változásának átadásával, ill. historikus adatainak SIEM rendszerek általi lekérde-

zésével. A konfigurációs adatok automatizált frissítését támogató konfigurációkezelési megoldások észlelik a konfigurációs elemekben és kapcsolataikban bekövetkezett változásokat, ezeket elemezhetik és a nem engedélyezett változásokat jelezhetik a konfigurációmenedzsernek, miközben naplózzák az eseményt. A naplófájlokat feldolgozó SIEM rendszerek észlelik a nem engedélyezett IT-infrastruktúra-változásokat, és ez alapján információbiztonsági eseményt jelenthetnek az adminisztrátoroknak.

Egy jól felépített és bevezetett IT-üzemeltetési modell és CMDB-re épülő támogató IT-szolgáltatásmenedzsment (Information Technology Service Management – ITSM) rendszer fontos szerepet játszik a felhasználói tevékenységek elemzésében, a szokatlan tevékenységek azonosításában és információbiztonsági események feltárásában.

10. LEHETSÉGES MŰKÖDÉSI MODELL FELHASZNÁLÓI TEVÉKENYSÉGEK AUTOMATIZÁLT ELEMZÉSÉRE

A SIEM rendszerek esetében a szokatlan események valós idejű azonosítása és riasztások küldése mellett – az üzemeltetés megkönnyítése érdekében – az adminisztráció mértékének minimalizálása is kulcsfontosságú feladat. Ez megfelelő működési modell kialakításával és a felhasználói profil kialakításához szükséges alapadatok partnerrendszerekből való automatizált feltöltésével, rendszeres frissítésével és automatikus lekérdezésével érhető el.

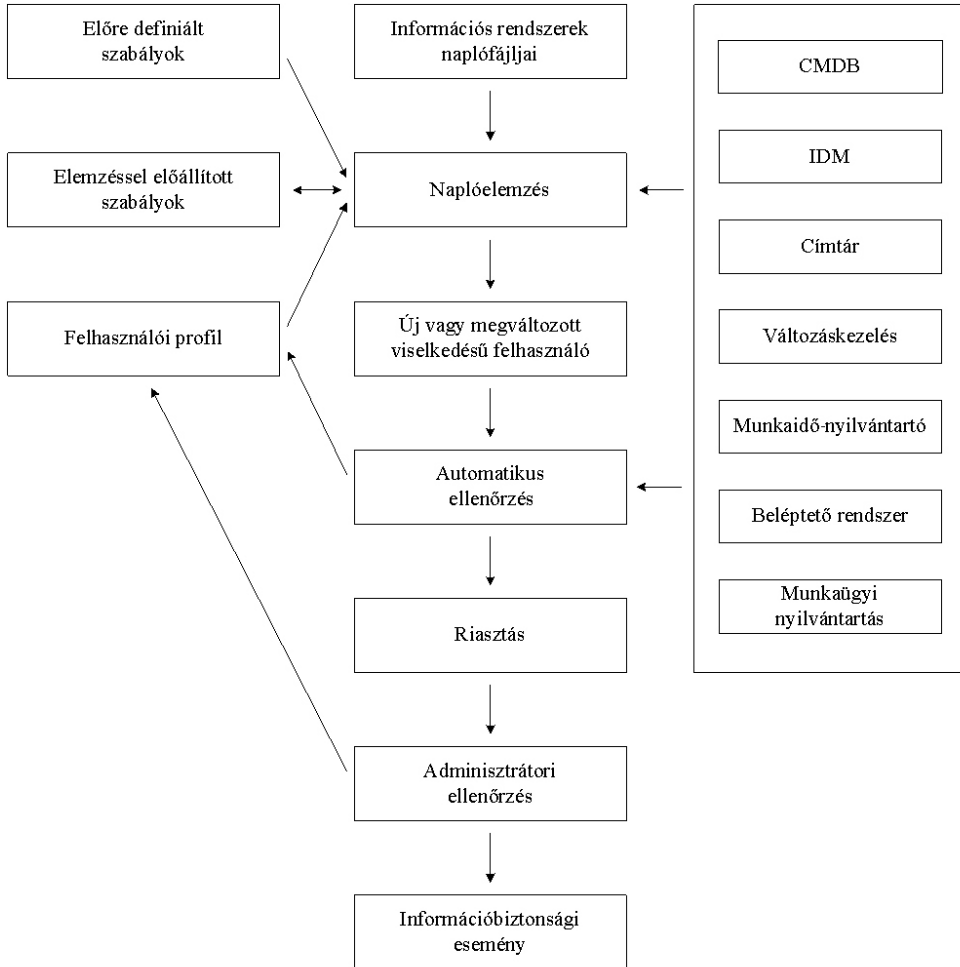
A modern SIEM rendszerekkel szemben követelmény, hogy kapcsolódási lehetőséget biztosítanak rendszerfelügyeleti és információbiztonsági megoldásokhoz,²⁰ mint pl. cím-tár, CMDB (Configuration Management Database – Konfigurációkezelési adatbázis), incidenskezelés, változáskezelés, IDS (Intrusion Detection System – Behatolásjelző rendszer), IPS (Intrusion Prevention System – Behatoláselhárító rendszer), vírusirtók, proxyszerverek, amelyek lekérdezésével felgyorsíthatják a naplófájlok feldolgozását, és javíthatják a szokatlan események meghatározásának pontosságát.

Ha megfelelően részletes naplóállományok állnak rendelkezésre, lehetőség nyílik az új és módosult felhasználók, szerepkörök és jogosultságok azonosítására. A rendelkezésre álló alapadatok lekérdezésével és felhasználásával azonosítható a létrehozás vagy módosítás jogsága. Ha nem áll rendelkezésre megfelelő mennyiségű és minőségű alapadat, a felhasználó- és szerepkör-módosításokat a rendszer szokatlan eseményként továbbíthatja az adminisztrátoroknak, akik azt elemezhetik és nyugtázzhatják mint új vagy megváltozott felhasználót, vagy azonosíthatják mint információbiztonsági eseményt. A szervezet infrastruktúrájának fejlettsége, a felhasználói tevékenységek elemzéséhez szükséges alapadatok informatikai rendszerekben való rendelkezésre állása jelentősen befolyásolja a beállítás és karbantartás során elvégzendő feladatok mennyiségét és az információbiztonsági események azonosítását. A naplóelemzések elvégzése során új adatok állhatnak elő a felhasználókról, ame-

²⁰ James TARALA: *Implementing the 20 Critical Controls with Security Information and Event Management (SIEM) Systems* – SANS Institute Infosec Reading Room, April 2011, 16. Forrás: www.sans.org/reading-room/whitepapers/analyst/implementing-20-critical-controls-security-information-event-management-siem-systems-34965 (2015. 07. 01.)

lyeket a hatékonyság érdekében a SIEM rendszernek historikusan kell rögzítenie, folyamatosan pontosítva azokat.

2. ábra • Automatizált felhasználóprofil-elemzési modell (saját szerkesztés)



A szervezetek többsége nem rendelkezik a felhasználói tevékenységek elemzéséhez szükséges alapadatok teljes körű elektronikus leképezésével, ezért számukra nem elérhető a felhasználói profil teljes körű elemzése. Kétféle megközelítés létezik ennek áthidalására:

- a hiányzó alapadatokhoz kapcsolható elemzések kihagyása, ami szokatlan események azonosításának elmaradásával és információbiztonsági események észlelésének elmulasztásával járhat;
- a hiányzó alapadatokhoz kapcsolható elemzések elvégzése és a kapcsolódó gyanús napló-bejegyzések esetén adminisztrátori riasztás küldése.

Mindkét megközelítésnek megvan a maga előnye és hátránya: ha nem teljes körű az elemzés, gyorsabban végrehajtható, de információbiztonsági események maradhatnak észrevétlenül, míg a hiányos adatokon futtatott elemzések több időbe telnek, pontatlanabbak és sok lehet a hamis riasztás, amely nagyobb adminisztrációs terhet jelent a szervezet számára. Nemcsak a két véglet létezik, minden szervezetnek meg kell találnia azok között azt a beállítást, amely azonosítja a számára jellemző információbiztonsági eseményeket, de nem jelent túl nagy adminisztrációs terhet a hamis riasztások kiszűrése során (2. ábra). A SIEM rendszerek bevezetésének tervezéséhez és kivitelezéséhez hasznos támogatást nyújt David Swift: *Successful SIEM and Log Management Strategies for Audit and Compliance*²¹ című tanulmánya.

11. FELHASZNÁLÓIPROFIL-ELEMZÉS A KÖZIGAZGATÁSBAN

A közigazgatásban sok intézmény kezel nagy mennyiségű személyes adatot, szolgálati titkot és államtitkot, amelyek hozzáférhetősége, sérülése és elvesztése kritikus lehet. A valós idejű felhasználóprofil-elemzés nagymértékben hozzájárulhat az adatok védelméhez. Ugyanakkor a felhasználóprofil-elemzés megvalósíthatóságának szempontjából fontos szerepet játszik a szervezet infrastruktúrájának fejlettsége, a rendelkezésre álló szakemberek tudása, az anyagi erőforrások rendelkezésre állása. Ezek az állami intézmények és szervezetek esetében sajátos képet mutatnak.

Gyakran előfordul, hogy az állami szervezetek költséghatékonyagra vagy pénzhiányra hivatkozva elhalasztják a szoftverek verziófrissítését, lecserélését újabb, modernebb megoldásokra. Az elavult technológiák jelentősen befolyásolhatják a felhasználói viselkedés elemzéséhez szükséges naplóbejegyzések rendelkezésre állását és a szükséges törzsdatok automatizált átemelését.

A bérezési modell miatt a nagyobb tudással rendelkező informatikai szakemberek egy része távozik a közigazgatásból, ezáltal folyamatos kihívás a megfelelő szaktudás biztosítása. Ez megnehezíti a magas szintű üzemeltetés fenntartásának folyamatosságát, és magas kockázatot jelent a kilépő munkatársak felhasználói jogosultságainak megszüntetése.

A költségvetési szervek gazdasági lehetőségei korlátozottak, rendszereik megújítása folyamatos kihívást jelent. Az információbiztságot jogszabály írja elő, amelynek megvalósítása folyamatosan zajlik. A kritikus rendszereket üzemeltető szervezetek esetében előírás a naplóelemző megoldás bevezetése.

A felsorolt feltételek mentén első generációs SIEM rendszerek megvalósítása magas bevezetési és fenntartási költségek miatt csak kevés szervezet számára volt elérhető.

A modern, automatizált törzsdatok-kezeléssel bíró és öntanuló felhasználóprofil-elemzést megvalósító SIEM rendszerek bevezetési és üzemeltetési költségei lehetővé teszik azok alkalmazását az állami szervezetek számára is. Automatizáltságukból adódóan üzemeltetésük kisebb szakmai felkészültség mellett is biztonságos, és a legnagyobb kihívást az elavult rendszerek naplózási hiányosságai jelentik.

21 David SWIFT: *Successful SIEM and Log Management Strategies for Audit and Compliance*, SANS Institute Infosec Reading Room, November 4, 2010, 40. Forrás: www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528 (2015. 07. 02.)

A naplózási hiányosságok megszűnhetnek az alkalmazásokkal szemben támasztott új vagy módosított ügyviteli igények megvalósítása során és új, korszerűbb rendszerek bevezetésével. A folyamatos fejlődésnek köszönhetően idővel megszűnnek a naplózási hiányosságok, de az időtáv fontos szerepet játszhat.

12. ÖSSZEFOGLALÁS

A tanulmány hangsúlyozza a felhasználóiprofil-elemzés szükségességét és sikeres alkalmazásának feltételeit. Számba veszi a szükséges eszközöket, és a hatékonyság növelésének lehetőségeit a rendelkezésre álló információk felhasználásával. Átfogó képet nyújt a szervezetek számára a sikeres megvalósítás feltételeiről, támogatva a bevezetésre való felkészülést. Javaslattal tesz egy lehetséges öntanuló felhasználóiprofil-elemzés modellre, amely lehetővé teszi a költséghatékony bevezetést és üzemeltetést, ezáltal a alkalmazhatóvá válik a közigazgatásban is. A bemutatott SIEM rendszerekbe integrált automatizált felhasználóiprofil-elemzés modell növeli a biztonsági naplóinformációk feldolgozását.

Az állami intézmények és államigazgatási szervek számára infrastruktúrájuk fejlettségétől függően a felhasználói elemzéssel kiegészített SIEM rendszer működtetése többek között az alábbi előnyöket nyújthatja:

- a felesleges jogosultságok és hozzáférések csökkentése,
- a rendszergazdai, üzemeltetői tevékenység kiemelt ellenőrzése,
- a szokatlan és információbiztonsági események azonosítása,
- munkatársak kényszerhelyzeti cselekvéseinek azonosítása és lojalitásának megfigyelése,
- felhasználói profilok illegális használatának azonosítása,
- lopott felhasználói azonosítókkal való visszaélés felderítése,
- információs rendszerek biztonsági hiányosságainak feltárása,
- információs rendszerek elleni, szervezeten belülről és kívülről érkező támadások felderítése és elhárítása,
- információszivárgás és -sérülés megakadályozása,
- működésfolytonosság növelése,
- biztonságtudatosági hiányosságok feltárása és kiküszöbölése,
- az eseményekben részt vevők egyértelmű azonosítása (az eseménymenedzsment, a felhasználóazonosítás és a konfigurációkezelés integrációja).

A SIEM rendszerek bevezetése és fenntartása akkor mondható sikeresnek, ha megvalósul az információbiztonsági események azonosítása minimális számú hamis riasztás mellett, és kezelhető, ill. még elfogadható terhet ró a biztonsági személyzetre.

SUMMARY IN ENGLISH: The implementation of information security in governmental institutions is regulated by law, which provides a complex regulation framework. The regulations emphasize the principle of least privilege, which means employees should be provided with necessary and sufficient access to do their jobs, while also requiring a

control system which limits their access to the execution of their tasks only. It also requires organizations handling large volume of personal data to carry out security analysis of the information systems' log files. Considering that the weakest link is the user, the most important aspect of log file processing is user activity analysis, building user profiles, identifying unusual events and analyzing them based on the available data. The paper discusses the goal, role, possibility, importance and limitations of building user profiles based on log files analysis, considering efficiency and inclusivity taking into account the need to minimize false alarms and administration workload. By the end of paper a cost-effective model is presented for automated user activity and profile analysis.

Dr. Michelberger Pál (michelberger.pal@kgk.uni-obuda.hu): Jelenleg egyetemi docens az Óbudai Egyetem Keleti Károly Gazdasági Karán, a Szervezési és Vezetési Intézetben. 1988-ban gépészmérnöki, 1997-ben pedig integrált menedzser – gazdasági mérnöki oklevelet szerzett a Budapesti Műszaki Egyetem Gépészmérnöki Karán. Doktori (PhD-) fokozatát a Zrínyi Miklós Nemzetvédelmi Egyetemen kapta katonai műszaki tudományokból 2005-ben. Értekezése honvédelmi célú informatikai rendszerelemek kiválasztásával és bevezetésével foglalkozott. 2015-ben az Óbudai Egyetemen habilitált. Tézisfüzetének címe: Információbiztonság és üzleti bizalom. Több mint 10 év iparvállalati gyakorlat után 2001-ben kezdett el a felsőoktatásban dolgozni. Volt a Gábor Dénes Főiskola, a Pannon Egyetem és a Budapesti Műszaki Főiskola oktatója is. Szakmai érdeklődése főleg az informatikai projektmenedzsmenthez, valamint a szabványos integrált (minőség-, környezet-, információbiztonsági) irányítási rendszerek kialakítási lehetőségeihez kapcsolható.

Dombora Sándor (dombora.sandor@kvk.uni-obuda.hu): Tanársegéd (Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, Híradástechnika Intézet). 1996-ban programtervező matematikus oklevelet, 1997-ben pedig integrált informatikai rendszerek szervezése és fejlesztése szakirányú mester fokozatot szerzett a Kolozsvári Babes-Bolyai Tudományegyetem Matematika és Informatika Karán. Pályafutását szoftverfejlesztéssel kezdte, majd adatbázis-szakértőként és üzemeltetési csoportvezetőként folytatta. Ezzel párhuzamosan többdimenziós adatbázisok témakörben kezdett kutatásokat, és adatbázis-kezelési gyakorlatot vezetett az Eötvös Loránd Tudományegyetemen. 2005-től kezdődően ITIL alapú üzemeltetési modellek kidolgozásával, IT-üzemeltetéstámogató rendszerek tervezésével és bevezetésével, valamint az optimális üzemeltetési folyamatok optimalizálásával foglalkozott. 2008-tól kezdődően információbiztonsági irányítási rendszerek kialakításával és bevezetésével kezdett foglalkozni. 2013-ban kezdett információbiztonsági és IT-üzemeltetési témákat oktatni az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Karán. 2015-től az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatója, kutatási témája az információbiztonsági irányítási keretrendszerek.

ÜGYFÉL-ELÉGEDETTSÉG MINT A HATÉKONYSÁG EGYIK DIMENZIÓJA

A közigazgatás teljesítménye jelentős mértékben meghatározza egy ország versenyképességét, ezért a teljesítmény mérése, értékelése, a teljesítményt befolyásoló tényezők feltárása kulcsfontosságú a közzférában ugyanúgy, mint az üzleti világban. A Jó Állam Jelentés 2015 a kormányzati képességeket hat hatásterületen méri, ezek egyike a hatékony közigazgatás (dimenziói: hozzáférhetőség, ügyfélteher, erőforrás-gazdálkodás, felkészültség, elégedettség). A tanulmány célja, hogy felhívja a figyelmet az ügyfélelégedettség-mérés szerepére és módszertanára a hatékony közigazgatás megvalósításában.

KULCSSZAVAK:

Jó Állam Jelentés, hatékonyság, ügyfél-elégedettség, mérés



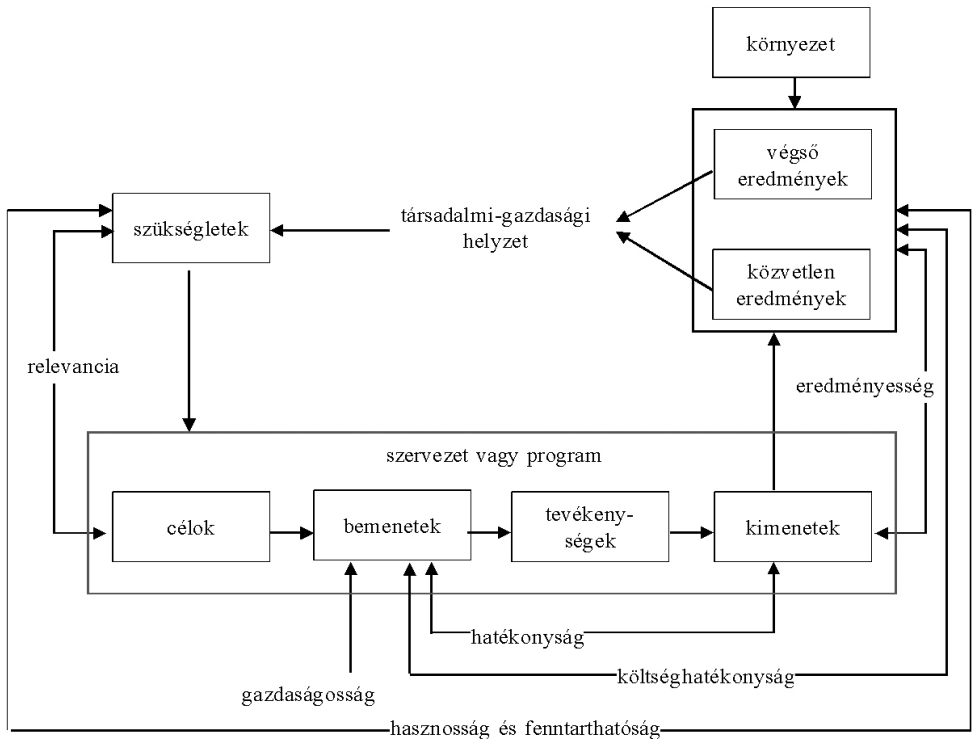
1. BEVEZETÉS

Az utóbbi két évtizedben a teljesítménymérés és -értékelés egyre nagyobb figyelmet kap a közigazgatásban. Számos nemzetközi (EU, ENSZ, OECD, IMD, WEF, Világbank) és hazai (KSH, ÁSZ, NKE) szervezet foglalkozik a kormányzati teljesítmény mérhetőségének a problémájával, kidolgozva különböző mérési és értékelési keretrendszereket.

A közigazgatás „jósága” (minősége) az elvárásoknak (célkitűzéseknek) való megfelelés mértékében értékelhető. A közigazgatás akkor tekinthető jónak (eredményesnek, hatékonynak, gazdaságosnak), ha a kimenetek, eredmények, hasznok megfelelnek a célkitűzéseknek (elvárásoknak) és a felhasznált erőforrások (bemenetek) nem haladják meg a szükséges mértéket. A teljesítmény összetevőit, azok kapcsolatrendszerét mutatja az 1. ábra.

A hatékonyságot a szakirodalom sokféleképpen értelmezi. A Magyar Zoltán Közigazgatás-fejlesztési Program (MP) célkitűzése a hatékony nemzeti közigazgatás megteremtése, ahol a hatékonyság hat szempont (eredményes, gazdaságos, hatásos, biztonságos, felüglyelhető és alkalmazkodó) egységeként értendő. Ezen elveknek a közigazgatás működésének minden területén meg kell jelenniük.

1. ábra • Teljesítményértékelési modell (Forrás: Van Dooren–Bouckaert–Halligan, 2010, 18)¹



Horváth M. Tamás (2005) a teljesítményt a gazdaságosság, hatékonyság, eredményesség és minőség tartalmakra bontja.² Értelmezésében a minőség az eredményességhez kapcsolódó, de annál szűkebb fogalom, amit a felhasználók által közvetlenül értelmezett paraméterek fejeznek ki. A közigazgatás szolgáltató jellegének megfelelően a teljesítmény egyik legfontosabb fokmérője az állampolgári elégedettség, ami a stratégiákban is megjelenik.

„A Magyar Program célja az ügyfelek igényeit és érdekeit figyelembe vevő, ügyfélközpontú szolgáltató működés kialakítása, az eljárások egyszerűsítése, az ügyfélterhek csökkentése és egységesen magas színvonalú, mindenki által hozzáférhető szolgáltatások kialakítása.”³

Nemeslaki András szerint a társadalmi jelenségeket folyamatosan kutatni kell, hogy érvényes és megbízható képet kapjunk róla. „A megmért eredmény tudatában dönthetünk úgy,

1 W. VAN DOOREN, G. BOUCKAERT, J. HALLIGAN: *Performance management in the public sector*, London, Routledge, 2010.
 2 HORVÁTH M. Tamás: *Közmenedzsment*, Budapest, Dialóg Campus Kiadó, 2005.
 3 Közigazgatási és Igazságügyi Minisztérium: *Magyar Zoltán Közigazgatás-fejlesztési Program (MP 11.0). A haza üdvére és a köz szolgálatára*, MP 11.0, 2011, 41. Forrás: magyarprogram.kormany.hu/admin/download/8/34/40000/Magyar-Kozigazgasat-fejlesztési-Program.pdf (2015. 10. 25.)

hogy változtatni szeretnénk valamin – ahhoz azonban, hogy megtudjuk, célhoz értünk-e vagy kudarcot vallottunk, ismét csak mérésre van szükség (hatásvizsgálat).⁴

Az ügyfélközpontú működés kialakításához és fejlesztéséhez ismerni kell az ügyfelek igényeit és a megvalósítás értékeléséhez mérni kell az ügyfelek elégedettségét, ami mutatók (indikátorok) segítségével történik.

Az indikátorok és modellek kiválasztása, használata, a felmérések tervezése és megvalósítása nagy körültekintést, szakértelmet igényel.

A teljesítményértékelési modellnek (1. ábra) az alábbi főbb területek indikátorai felelnek meg:

- célok, szükségletek,
- bemenetek (szolgáltatási kapacitások, erőforrások, költségek),
- kimenetek (szolgáltatás kibocsátása),
- eredmények, hatások,
- gazdaságosság,
- hatékonyság,
- eredményesség.⁵

Az ügyfél-elégedtség területét

- a szolgáltatás minőségére vonatkozó ügyfél- (igénybevevői) elvárások (célok, szükségletek), szakmai specifikációk, valamint
- az eredményesség ügyfél általi (igénybevevői) értékelése jellemzi.

Bár az ügyfelek véleménye nem pontosan tükrözi a tényleges teljesítményt, a méréshez alkalmazott indikátoroknak a teljesítményértékelési rendszer részeként teljesíteniük kell a SMART⁶ és a QQTTP⁷ kritériumrendszer követelményeit.

2. ÜGYFÉLELEGEDETTSÉG-MÉRÉS⁸

Az elégedettségmérés szempontjából azonosítani kell, kit tekintünk ügyfélnek. A Ket. szerint „Ügyfél az a természetes vagy jogi személy, továbbá jogi személyiséggel nem rendelkező szervezet, akinek jogát vagy jogos érdekét az ügy érinti, akit hatósági ellenőrzés alá vontak, illetve akire nézve a hatósági nyilvántartás adatot tartalmaz.”⁹ Tágabb értelemben ügy-

4 NEMESLAKI A. et al: *E-közzolgálatfejlesztés. Elméleti alapok és kutatási módszerek*, Budapest, Nemzeti Közzolgálati Egyetem, 2014, 28.

5 szerk. GÁSPÁR Máttyás: *Mindenki fontos! A helyi közösségi önkormányzás esélyei, a közmenedzsmnt új irányai*, Budafok-Tétény, Budapest XXII. Kerület Önkormányzat, 2011, 272–275. (részletes indikátorrendszert határoz meg a helyi közigazgatásra vonatkozóan)

6 SMART: Specific (specifikusak), Measurable (mérhetőek), Available/Achievable (elérhetőek, rendelkezésre állnak), Relevant/Reliable (relevánsak, megbízhatóak), Timely (aktuálisak)

7 QQTTP: Quantity (mennyiség), Quality (minőség), Time (idő), Target group (célcsoport), Place (hely)

8 A fejezetnek nem célja a teljes módszertan és technika áttekintése, amihez bőséges irodalom áll rendelkezésre. Ilyenek például: GAJDUSCHEK György: *Módszertani útmutató a hivatali ügyfél-elégedtség méréséhez*, MKI, Budapest, 2005.

7/A munkacsoport: *Módszertani útmutató az ügyfélelégedtség-mérésre és az ügyfélkarta készítésére*, ÁROP 1.2.18 – Szervezetfejlesztési Program, KIM–KIH, 2013. Forrás: magyaryprogram.kormany.hu/download/e/a3/70000/7_A_ugyfelelegedettseg_meres_modszertan.pdf (2015. 10. 08.)

9 2004. évi CXL. törvény közigazgatási hatósági eljárás és szolgáltatás általános szabályairól, 15. § (1).

félnek tekinthetünk mindenkit, aki kapcsolatba kerül a közigazgatási szervezettel. Az ügyfelek lehetnek például:

- állampolgárok, vállalkozások;
- hazai és külföldi ügyfelek;
- belső és külső ügyfelek.

Az ügyfél-elégedettség az ügyfél megítélése arról, hogy a közszolgáltatással szembeni követelményei (elvárásai) – általában, vagy egy adott területen – milyen mértékben teljesültek.

A szolgáltatások minőségének a mérésére dolgozták ki a SERVQUAL (SERVice QUALity) modellt, amellyel meghatározható az elvárt (ideális) és a tényleges szolgáltatási szint, valamint annak a fontossága az ügyfél szempontjából.

A SERVQUAL modell megalkotói a szolgáltatások minőségének kezdetben tíz dimenzióját (kompetencia, udvariasság, hitelesség, biztonság, hozzáférés, kommunikáció, alkalmazkodóképesség, tárgyi eszközök, megbízhatóság, interaktivitás) határozta meg,¹⁰ amit később ötre redukáltak (tárgyi eszközök, megbízhatóság, alkalmazkodóképesség, hitelesség, empátia).^{11, 12}

Az ügyfél-elégedettség más dimenziók szerint is mérhető. Gáspár Mátyás (2011) szerint az ügyfél akkor elégedett a hivatallal, ha az elérhető, kiszámítható, rendeltetésszerű, empatikus, személyes, szakszerű, törvényes, igazságos, egyszerű, komfortos, gyors, hatékony, időszzerű, segítőkész, pénzkímélő, kulturált hagyományos értelemben, digitálisan kulturált.¹³ A szerző a szolgáltatás minőségével kapcsolatos ügyfélelvárásoknál és szakmai specifikációknál a hitelesség, megbízhatóság, komfort, teljesség, hozzáférés, alkalmazkodás, gyorsaság, szakszerűség, biztonság, udvariasság, kommunikáció, kapcsolat jellemzőket hangsúlyozza.¹⁴ A vizsgált jellemzők (szűkebb vagy tágabb) körét a felmérés céljával összhangban célszerű kiválasztani.

A SERVQUAL modell az elvárt és a tényleges szolgáltatási szint közötti különbségek, rések feltárását is megcélozza. Az eltéréseket az ún. GAP-módszer több részre bontva vizsgálja:

- az ügyfél elvárása és a szervezet vezetésének az ügyfélelvárásokra vonatkozó elképzelése közti rés;
- a szervezet vezetésének az ügyfélelvárásokra vonatkozó elképzelése és a szolgáltatás jellemzői közti rés;
- a szolgáltatás jellemzői és a szolgáltatásnyújtás közti rés;
- a szolgáltatásnyújtás és ennek kifelé való kommunikációja közti rés;
- az ügyfél elvárása és a szolgáltatásnyújtás közti rés;
- az ügyfél elvárása és az alkalmazottak ügyfélelvárásokra vonatkozó elképzelése közti rés;
- az alkalmazottak elképzelése és a vezetés elképzelése közötti rés.¹⁵

10 A. PARASURAMAN et al.: *A conceptual model of service quality and its implications for future research*, The Journal of Marketing, Fall, 1985, 41–50.

11 W. J. KETTINGER, C. C. LEE: *Perceived service quality and user satisfaction with the information services function*, Decision Sciences, 25(1995)/5–6, 737–765.

12 L. F. PITT, R. T. WATSON, C. B. KAVAN: *Service quality: A measure of information systems effectiveness*, MIS Quarterly, 19(1994)/2, 173–188.

13 GÁSPÁR Mátyás: *i. m.*, 90.

14 *Uo.*, 273–274.

15 Kibővített GAP modell. Parasuraman 1985-ös eredeti modelljében 4 rés szerepelt, amit Curry 1992-ben, Luk & Layton 2002-ben kiegészített.

Az ügyfelek szempontjából az 5. rés (az ügyfélelvárások és tapasztalatok közötti különbség) feltárása és mértékének csökkentése a legfontosabb.

A SERVQUAL modell később más mérési rendszerekbe is beépült. DeLone és McLean 2003-ban frissített információs rendszer sikermodellje (D&M IR sikermodell)¹⁶ hat dimenzióra bontva, azok kapcsolatait azonosítva méri a rendszer minőségét. D&M szerint az információs rendszer, az információ és a szolgáltatás minősége egyaránt hat a felhasználói elégedettségre, a használatra/használati szándékra, és így ezek alapján a hasznosságra. A D&M IR sikermodell e-kereskedelmi mérőrendszerében a szolgáltatás minőségét a bizalom, empátia és reagálóképesség jelzi, míg az elégedettséget a vásárlások megismétlése, a látogatások megismétlése és a felhasználói felmérések eredményei fejezik ki. Közigazgatásra vonatkoztatva a felhasználói elégedettség másként értelmezhető. Az ismételt ügyintézés nem utal az elégedettségre. Ismert tény, hogy az állampolgárok, vállalkozások és szervezetek képviselői nem kívánnak a közigazgatási szervezetekkel kapcsolatot tartani, ügyet intézni, de rákényszerülnek. Éppen ezért az ügyfelek természetes ellenérzése (előítélete) eleve negatívan hat elégedettségükre.

A közigazgatási szervezeteknek a minőségmenedzsment-rendszerek követelményeinek megfelelően rendszeres, összehasonlítható eredményességi és elégedettségi vizsgálatokat kell végezniük. Általában jellemzőek az egy-egy szerv működésével kapcsolatos véleményfelmérések, de átfogó, országos felmérésekre ritkán kerül sor.

Tíz évvel ezelőtt a Miniszterelnöki Hivatal kezdeményezésére egy országos közvéleménykutatás indult az ügyfelek közigazgatási ügyintézással kapcsolatos elégedettségének, illetve fejlesztési igényeinek a felmérésére, a lakosság és a vállalkozások körében. A válaszok kiértékeléséből kiderült, hogy az elégedettségre több tényező is hat. Ilyenek például a lakóhely, kor, nem, képzettség, jövedelmi helyzet/vállalat nagysága, technológiai felkészültség. Az igények felmérése nyitott és zárt kérdésekkel valósult meg. Nyitott kérdéseknél a választ az ügyfeleknek kellett megfogalmazni, míg a zárt kérdéseknél a felajánlott jellemző fontosságát kellett jelezni. Az igények többsége akkor az ügyintézés gyorsítására és egyszerűsítésére vonatkozott. Tíz évvel ezelőtt az e-közigazgatás még gyerekcipőben járt, de az ügyfelek már ekkor is igényelték a teljes körű elektronikus ügyintézés lehetőségét több ügyfajta esetén is.¹⁷

16 W. H. DELONE, E. R. MCLEAN: *The DeLone and McLean Model of Information Systems Success: A Ten-Year Update*, Journal of Management Information Systems, 19(2003)/4, 9–30.

17 Marketing Centrum: *A közigazgatási ügyintézés társadalmi megítélése – 2005*. Forrás: www.palyazat.gov.hu/doc/585 (2015. 11. 02.)

M.Á.S.T. Piac- és közvéleménykutató társaság: *A magyar lakosság közigazgatási ügyintézással kapcsolatos attitűdjeinek vizsgálata – 2006*. Forrás: www.palyazat.gov.hu/doc/589 (2015. 11. 02.)

Fact Intézet: *A közigazgatási ügyintézés társadalmi megítélése a magyarországi vállalkozások körében – 2006*. Forrás: www.palyazat.gov.hu/doc/590 (2015. 11. 02.)

KÖZIG IH: *A közigazgatási barométer változóan felhős időt jelez – avagy az ügyfelek elégedettsége a közigazgatási ügyintézással – 2006*. Forrás: www.palyazat.gov.hu/doc/591 (2015. 11. 02.)

3. A JÓ ÁLLAM JELENTÉS HATÉKONY KÖZIGAZGATÁS HATÁSTERÜLETE

A Nemzeti Közszerológiai Egyetem kutatói kiemelten foglalkoznak a kormányzati hatékonysággal.¹⁸ A Kaiser Tamás vezetésével működő Jó Állam Kutatóműhely több tudományterület tudósait és szakembereit¹⁹ összefogva vizsgálja a modern állam, a hatékony közigazgatás összetevőit és azok mérhetőségét. A kutatóműhely célja a magyar kormányzati hatékonyság változását, fejlődését kifejező, módszertanilag és statisztikailag megalapozott mutatórendszer kidolgozása.²⁰ A Jó Állam Jelentés 2015 a kormányzati képességeket 6 hatásterületen méri, hatásterületenként 5 dimenziót, dimenzióként 5 (1 fő és 4 rész) indikátort meghatározva.

A jelentés hatásterületei:

- biztonság és bizalom a kormányzatban,
- közösségi jóllét,
- pénzügyi stabilitás és gazdasági versenyképesség,
- fenntarthatóság,
- demokrácia,
- hatékony közigazgatás.

A jelentés közvetlenül mérhető mennyiségi jellemzők mellett közvetlenül nem mérhető minőségi jellemzőket is vizsgál.

A kemény adatok jól mérhetők és számszerűsíthetők (pl. ügytípusok száma, illeték mértéke).

A puha adatok szubjektívebbek és nehezebben számszerűsíthetők (pl. bizalom, elégedettség), amelyek forrása lehet a KSH reprezentatív lakossági adatgyűjtése, vagy akár kérdőíves felmérés is.

A társadalomtudományi elemzéseknél – a közigazgatás hatékonyságának a vizsgálatánál is – elkerülhetetlen a puha mutatók felhasználása, hiszen nem minden jelenség írható le egyértelműen mérhető jellemzőkkel, illetve a számszerűsítést bizonytalanság, értelmezési problémák, szubjektivitás befolyásolhatja.

A közigazgatás hatékonyságát a jelentés 5 dimenzióra bontva vizsgálja:

- Hozzáférhetőség: a közigazgatási szolgáltatásokhoz való hozzáférés mérése keresleti és kínálati oldalról, figyelembe véve a többcsatornás elérést és a szolgáltatások különböző fejlettségi szintjét.
- Ügyfélteher: adminisztratív terhek azonosítása és **mérése**, ami egyaránt **érinti** az ügyintézési időt, a szolgáltatási díjakat és a tehermentesítő szolgáltatásokat.
- Erőforrás-gazdálkodás: a felhasznált erőforrások (pénz, eszköz, emberi erőforrás) hatékonyságának a mérése.

18 Az NKE gondozásában 2014-ben több tanulmány is megjelent a témában. Pl. szerk. KAISER T. – KIS N.: *A jó állam mérhetősége*; szerk. KAISER T.: *Hatékony közszerológiai és jó közszerológiai – Nemzetközi és európai dimenziók*; VÉRTES L.: *Az állami beavatkozás joga és hatékonysága*.

19 A kutatási területek vezetői: Dr. Kis Norbert, Prof. Dr. Báger Gusztáv, Prof. Dr. Csath Magdolna, Besenyey Mónika, Dr. Fejes Zsuzsanna, Dr. Kádár Krisztián.

20 A nemzetközi felmérések az országok összehasonlítását, rangsorok felállítását támogatják, általában komplex indexek kidolgozásával.

– Felkészültség: a humánerőforrás *képzettségének, szakmai hozzáértésének és motiváltságának a mérése.*

– Elégedettség: az ügyfelek igényeinek és elvárásainak a felmérése, leírása.

Az elégedettség dimenzióhoz jelenleg még nem állnak rendelkezésre adatok, a mérés és értékelés a jelentés következő verziójában jelenhet meg. A tervezett országos lekérdezés csak az állampolgárokat célozza meg (1500 fős reprezentatív nagyminta) és azt vizsgálja, hogy az állampolgárok mennyire ismerik, értik és használják a közigazgatást, az megfelel-e az igényeknek, elvárásaiknak, elképzeléseik és tapasztalataik alapján mennyire elégedettek a közigazgatással.

Az elégedettség dimenzió tervezett indikátorai (puha mutatói):

- ügyfél-elégedettségi index,
- elégedettség a hozzáférhetőséggel,
- elégedettség az adminisztratív terhek mértékével,
- elégedettség az erőforrások hatékonyságával,
- elégedettség a felkészültséggel.

Az *ügyfél-elégedettségi (fő) index* összefoglalóan, komplex mutatóval fejezi ki az igénybevevők közigazgatással szemben támasztott elvárásainak (vagy azok egy részének) a teljesülését. A kapott eredmény nagyban függ attól, hogy milyen elvárásokat vizsgálunk (pl. a SERVQUAL dimenziói közül választva). Éppen ezért célszerű az egyes tényezőknél az elégedettség mértéke (elvárások teljesülése) mellett az adott jellemző fontosságának mértékét is meghatározni. Az átlagos elégedettségi index így a fontossággal súlyozott elégedettségi szint alapján számítható ki. A mutató korosztály, képzettség, terület stb. szerinti bontásban további információkat nyújthat a tervezett fejlesztésekhez.

Az elégedettség további tervezett mutatói a hatékony közigazgatás hatásterület 1–4. dimenziójához kapcsolódnak.

A *hozzáférhetőség* több szempont alapján is értékelhető:

- hely: ügyfélszolgálati szervezeti egységek földrajzi elhelyezkedése (az igénybevételhez mekkora utat kell megtenni);
- idő: ügyfélszolgálatok időbeli rendelkezésre állása;
- ügkörök száma: különböző csatornákon és szervezeteknél intézhető ügkörök száma;
- elektronikus szolgáltatások aránya és szintje;
- esélyegyenlőség és akadálymentesség biztosítása a szolgáltatások elérése során.

A *hozzáférhetőség index* komplex mutatóként (súlyozott átlagként) fejezheti ki az egyes szempontok megvalósításával kapcsolatos igények teljesülésének a mértékét.

Az *adminisztratív terhek*²¹ mértéke szintén több területen vizsgálható:

- ügyintézési idő: az állampolgárok ügyintézésre fordított ideje alapján (problémát jelenthet az ügyintézés és az ügyintézési idő eltérő értelmezése, illetve a bázisadat meghatározása);

21 Az EUPAN tanulmánycsoportja által kidolgozott lakossági SCM (Standard Cost Model) modell alapján elérhető a lakossági adminisztratív teher nagyságának mérésére szolgáló módszertan. Ennek értelmében az állampolgárok adminisztratív terheit költségben, illetve időráfordítás alapján lehet meghatározni.

- szolgáltatási díjak: az ügytípusok jogszabályban rögzített eljárási illetékei és szolgáltatási díjai (az ügyfél az ügyintézés költségeibe beleértheti az utazás költségeit, vagy éppen az ügyintézés miatt elmaradt bevételeit);
- eljárások: pontosabb tájékoztatás, hatósági eljárások átszervezése és leegyszerűsítése, az elektronikus lehetőségek kiterjesztése és a kapcsolódó jogszabályok leegyszerűsítése a MP egyszerűsítési programja²² alapján.

A bürokráciacsökkentés (az ügyintézési idő és a szolgáltatási díjak csökkentése, és az eljárások leegyszerűsítése) az egyének szintjén különbözően érzékelhető,²³ de maga a tény biztosan magas elégedettségi szintet eredményez.

Az *erőforrás-hatékonyság* a szervezet működését jellemzi. Habár a közpénz elköltése általában érdeklő az állampolgárokat, de a felhasznált erőforrások (pénz, eszköz, emberi erőforrás) mértéke és hatékonysága általuk kevésbé ismert, így az elégedettségi szint mérése ezzel a területtel kapcsolatosan nem javasolt. Célszerű lenne ehelyett más ügyintézési elemmel kapcsolatos véleményt kérni (ilyenek lehetnek például az ügyintézéssel kapcsolatos információk rendelkezésre állása, a közigazgatási portálok ismertsége, használhatósága).

A közigazgatásban foglalkoztatottak *felkészültsége* elsősorban a szakszerűségben jelenik meg az ügyfelek számára. Számukra az a fontos, hogy hozzáértő, az adott területen megfelelő szakmai ismeretekkel, tudással, jártassággal rendelkező dolgozókkal kerüljenek kapcsolatba. A közigazgatásban foglalkoztatottaktól, főleg az ügyfélszolgálatot ellátó személyektől az ügyfelek szakszerűséget (hibamentes szolgáltatást), alkalmazkodóképességet (empátiát) és udvariasságot várnak el. Célszerű ezen tényezőket külön-külön megvizsgálni, értékelni.

4. ÖSSZEGZÉS, JAVASLATOK

Megfigyelhető, hogy nemzetközi és hazai viszonylatban is kiemelt szerepet kap a kormányzati *hatékonyság* mérésének az igénye, de jelentős eltérések tapasztalhatók a vizsgált témaköröket, módszereket és indikátorokat illetően. A *Jó Állam Jelentés* a hazai kormányzati hatékonyság, és ezzel kapcsolatosan a közigazgatási hatékonyság időbeli fejlődését kívánja mérni. A hatékony közigazgatás fejezet azonban jelenleg nem teljes, mert az elégedettségmérés adatai még nem állnak rendelkezésre. A kutatóknak most azt kell eldönteniük, hogy milyen jellemzőket, elemeket kell mérni, hogy megismerjék az állampolgároknak a közigazgatási hatékonysággal kapcsolatos általános elégedettségi szintjét, illetve egy-egy területről kialakított véleményét.

Teljesítménymenedzsment nézőpontból kiindulva látható, hogy a hatékonyság fogalmat többféle (szűkebb és tágabb) értelmezésben használják a kutatók. A teljesítmény minőségi eleme az ügyféligények és ügyfél-elégedettség meghatározása, mérése. Az ügyfél-elégedettség-mérés módszertanának SERVQUAL modellje (illetve az azt beépítő D&M IR sikermo-

22 MP Egyszerűsítési Programja. Forrás: magyaryprogram.kormany.hu/egyszerusitesiprogram (2015. 10. 28.)

23 Függs az adatgyűjtés időpontjától is. Más értékeket kapunk, ha közvetlenül az ügyintézés befejezése után kérdezzünk rá, mintha egy későbbi időpontban. Az elégedettség mértékét erőteljesen befolyásolja az ügyfél lelkiállapota is.

dell) hasznos eszköz lehet az igények, specifikációk és elvárások, illetve azok közötti különbségek mérésére. A Jó Állam Jelentés hatékony közigazgatás hatásterületének dimenziói számos tényezőre, elemre bontva vizsgálhatók. Kiderült, hogy az elégedettségmérés tervezett indikátorai további kutatásokkal pontosíthatók, figyelembe véve az ügyintézés egyes aspektusainak, területeinek a minőségi jellemzőit. Az ügyfél-elégedettség több szempont együttes figyelembevételére alapján, komplex mutatókkal jellemezhető.

Az ügyfél-elégedettség mértéke a hatékonyság szempontjából meghatározó mutató, a felmérés eredményei egyaránt fontosak a kormányzat és az állampolgárok számára, hiszen az eredmények folyamatba integrálásával megalapozhatók a jövőbeli közigazgatási fejlesztések.

• • • • • • • • • •

SUMMARY IN ENGLISH: In the business sector it is crucial to measure and assess performance and to explore factors that influence it. It is not different in the public sector, because the competitiveness of a country highly depends on the quality of its services. The Good State and Governance Report 2015 measures governmental abilities in six impact areas. One of them is effective public administration (dimensions: accessibility, administrative burden, resource efficiency, preparedness, satisfaction). The aim of this study is to draw attention to the role of the customer satisfaction measurement and its methodology, because it is a determining factor in the process to realize effective public administration.

Dr. Orbán Anna (Orban.Anna@uni-nke.hu): a Nemzeti Közzolgálati Egyetem Közigazgatás-tudományi Kar E-közzolgálati Fejlesztési Intézet, Közzolgálati Informatika Tanszék adjunktusa és a Nemzeti Közzolgálati Egyetem Közigazgatás-tudományi Doktori Iskola hallgatója. Közgazdász, majd informatikatanári végzettséggel kezdett a Nemzeti Közzolgálati Egyetem Közigazgatás-tudományi Karának elődintézményén, az Államigazgatási Főiskolán oktatni 1986-ban. Azóta foglalkozik a közigazgatási informatikával, a közigazgatás és az informatika intenzíven fejlődő és átalakuló interdiszciplináris területével. Kutatási területe: e-közigazgatás, információs rendszerek, hatékonyság mérése.

A KÖZIGAZGATÁS ÉS A MÉDIA KAPCSOLÓDÁSI PONTJAI¹

A közigazgatás és a média kapcsolata két vonatkozásban is értelmezhető. Az egyik a közigazgatás működésének átláthatósága, média (közvetve a társadalom) általi kontrollja, ami nemcsak a demokratikus berendezkedés egyik alapja, de fontos alapköve a modern, elektronikus eszközökkel támogatott szolgáltató közigazgatás működésének is. Tisztázandó kérdés azonban, hogy meddig terjed e nyilvánosság, mennyiben jelent mást a közigazgatás (egészének) átláthatósága és az egyes közigazgatási eljárások nyilvánossága. A másik aspektus arról szól, hogy a közigazgatás milyen felügyeletet gyakorol a média működése felett, és hogy a felügyeleti rendszer szabályozása tekintetbe veszi-e a média által ellátott alkotmányos szerepet. A tanulmányban e kérdésköröket tekintjük át.

KULCSSZAVAK:

döntés megalapozását szolgáló adat, fogyasztóvédelem, iratbetekintés, közérdekű adat, hatósági ellenőrzés nyilvánossága, médiafelügyelet



1. ALAPVETÉS

Az állami működés átláthatósága, az állami szervek tevékenységével és a közpénzek felhasználásával kapcsolatos információk megismerhetősége nemcsak a társadalmi nyilvánosság² és a demokratikus berendezkedés egyik alapja,³ de fontos alapköve a modern, elektronikus eszközökkel támogatott szolgáltató közigazgatás működésének is.

Fontos és tisztázandó kérdés azonban, hogy meddig terjed e nyilvánosság, mennyiben jelent mást a közigazgatás átláthatósága és az egyes közigazgatási eljárások átláthatósága, és hogy mely alkotmányos elvek és konkrét szabályok mentén lehetséges a határvo-nal meghúzása.

1 E tanulmányt a szerzők a 650 éves Pécsi Tudományegyetem tiszteletére ajánlják.

2 GÁLIK Mihály, POLYÁK Gábor: *Médiaszabályozás*, KJK–Kerszöv, Budapest, 2005, 86.

3 Az „állami szervek és a végrehajtó hatalom nyilvánosság előtti működése a demokratizmus egyik alapköve, a jogállami államberendezkedés garanciája” [34/1994. (VI. 24.) AB-hat.]

A közigazgatás és a média kapcsolatának vizsgálata azért is különösen érdekes, mert a polgárok a közigazgatás működéséről a legritkább esetben tájékozódnak hivatalos iratokból, dokumentumokból, vagy a közigazgatási szervek által közölt információkból. A közigazgatás szervezetével, működésével kapcsolatos információk jellemzően a tömegtájékoztatás segítségével jutnak el az emberekhez.⁴

A közigazgatás és a média kapcsolata két vonatkozásban is értelmezhető. Az egyik, amint itt a bevezetőben utaltunk rá, a közigazgatás működésének átláthatósága, média (közvetve a társadalom) általi kontrollja, míg a másik aspektus arról szól, hogy az állami szervezetrendszer milyen felügyeletet gyakorol a média működése felett, és hogy a felügyeleti rendszer szabályozása tekintetbe veszi-e a média által ellátott kontrollfunkciókat. Tanulmányunkban e kérdésköröket tekintjük át.

2. A KÖZIGAZGATÁS MŰKÖDÉSÉNEK ÁTLÁTHATÓSÁGA

2.1. A közigazgatás működésének megismerhetősége

Az állami működés átláthatóságának legfontosabb, alapjogi szinten is védelemben részesített eszköze az információs szabadság, a közérdekű adatok megismerésének és terjesztésének szabadsága. Az Alaptörvény VI. cikk (2) bekezdése kimondja, hogy „[m]indenkinek joga van [...] a közérdekű adatok megismeréséhez és terjesztéséhez.” A szabályozás részletei az információs önrendelkezési jogról és az információs szabadságról szóló 2011. évi CXII. törvényben (Infotv.) található.

A törvény a közérdekű adat fogalmát igen tágan határozza meg, eszerint a – közigazgatási szerveknél tágabb alanyi kört jelölő – „közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől”.⁵

Az információs szabadság az egyén oldalán olyan jogot keletkeztet, ami az állam arra irányuló tevőleges kötelezettségét is jelenti, hogy biztosítsa ezeknek az adatoknak a nyilvánosságát.⁶ Az Infotv. kifejezetten is kimondja, hogy a közfeladatot ellátó szerv a feladatkörébe tartozó ügyekben köteles elősegíteni és biztosítani a közvélemény pontos és gyors tájékoztatását.⁷ Ennek alapvetően két úton lehet eleget tenni: vagy proaktív módon nyilvánosságra hozva egyes adatokat, vagy közérdekű adat igénylése esetén az igénylő rendelkezésére bocsátásával. A részletes szabályok áttekintése nélkül azt mondhatjuk, hogy ugyan az utóbbi időben sajnos egyértelmű tendencia a közérdekű adatokhoz való hozzáférés jogalkotással törté-

4 Lennard LUNDQUIST: *Az információ szabadsága és a svéd modell = Közszolgálat és etika*, szerk. GULYÁS Gyula, Helikon, Budapest, 1997, 208.

5 Infotv. 3. § 5. pont

6 GÁLIK-POLYÁK: *i. m.*, 87.

7 Infotv. 32. §

nő szűkítése,⁸ az elmúlt bő két évtizedben egy kiterjedt joggyakorlattal rendelkező és alapvetően rendeltetésszerűen működő jogintézmény jött létre, amely alkalmas a funkciója betöltésére, és ebben mind a médiának (különösen az oknyomozó újságíróknak), mind számos, e területre fókuszáló civil szervezetnek jelentős szerepe van.

2.2. A nyilvánosság korlátai

A tanulmány szempontjából leginkább érdekes kérdés az, hogy hol vannak a megismerhetőség korlátai, különösen az egyes konkrét közigazgatási eljárásokkal kapcsolatban, és mennyire koherens e terület szabályozása. Az Infotv.-ből kiindulva három korlátot, a személyes adatok és az üzleti titok védelmét, és a döntés megalapozását szolgáló adat megismerésének korlátait érdemes vizsgálni.⁹

A jogalkotó már a közérdekű adat fogalmának megalkotásakor világossá tette, hogy a személyes adatok megismerhetősége e körbe nem tartozik bele, annak védelme így főszabályként elsőbbséget élvez. Ez alapján tehát nem minősülnek közérdekű adatnak a közigazgatás azon nyilvántartásai, amelyek személyes adatot tartalmaznak, valamint bármely egyedi ügyben (közigazgatási eljárásban) az összes, természetes személlyel kapcsolatba hozható adat.¹⁰ Ugyancsak elsőbbséget élvez az üzleti titok védelme, feltéve, hogy az nem közpénzfelhasználással kapcsolatos.¹¹ Ez jelen tanulmány szempontjából azért lehet érdekes, mert előfordulhatnak olyan hatósági eljárások, ahol egyes iratok a jogi személy ügyfelek üzleti titkát képezhetik.

A közigazgatási eljárások jelentős része ugyanakkor nem, vagy alig érint személyes adatokat és/vagy üzleti titkot, így az ezzel kapcsolatos szabályozás önmagában még egyáltalán nem jelenti azt, hogy egyes (akár folyamatban lévő) ügyek részletei ne lennének megismerhetőek a közérdekű adatok megismeréséhez való jog alapján. A nyilvánosság korlátozására bizonyos esetekben azonban kétségkívül szükség van. A közérdekű adatok megismeréséhez való jog alkotmánybírósági értelmezésében is egészen korán megjelent az a gondolat, miszerint „garanciális intézménye a köztisztviselői munka színvonalának és hatékonyságának, hogy a köztisztviselők döntés-előkészítése szabadon, informálisan és a nyilvánosság nyomásától mentesen folyik. Ezért az aktanyilvánosság a közbülső munkaanyagokra nem, hanem csak a végeredményre vonatkozik.”¹²

A belső használatra készült, döntés-előkészítéssel kapcsolatos adatok (pl. munkaanyagok, emlékeztetők, tervezetek, vázlatok, javaslatok, a szervezeten belül váltott levelek)¹³ nyil-

8 Példaként említhetők a „számlaszintű” ellenőrzésre vonatkozó szabályok, az adatigénylő nevének kötelező megadása, a költségtérítéssel és a döntés megalapozását szolgáló adatokkal kapcsolatos változások.

9 Az információs szabadság további jelentős korlátját képezik a minősített adatok.

10 Ugyanakkor e szabály alól is több kivétel van, a törvény előírhatja bizonyos személyes adatok vagy nyilvántartások megismerhetőségét. Előbbire példa lehet a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy közfeladat-ellátással összefüggő személyes adata [Infotv. 26. § (2)], utóbbira a személyes adatokat is tartalmazó ingatlan-nyilvántartás.

11 Infotv. 27. § (3) bekezdés

12 34/1994. (VI. 24.) AB-határozat

13 12/2004. (IV. 7.) AB-határozat

vánosságát kizáró rendelkezések 1995-ben tételes jogi szabályként is megjelentek, amelyet több, alapvetően az Alkotmánybíróság elmarasztaló határozatai nyomán történt módosítás és pontosítás követett. Az Infotv. 27. § (5)–(6) bekezdésében található hatályos szabályozás szerint a közfeladatot ellátó szerv feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló adat a keletkezésétől számított tíz évig nem nyilvános. Ugyanakkor a szerv vezetője a megismerést – mérlegelve a megismeréséhez és annak kizárásához fűződő közérdek súlyát – engedélyezheti. A titkosság a döntés meghozatala után csak kivételesen tartható fenn, akkor, ha az adat további jövőbeli döntés megalapozását is szolgálja,¹⁴ vagy az adat megismerése a szerv törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását, így különösen az adatot keletkeztető álláspontjának a döntések előkészítése során történő szabad kifejtését veszélyeztetné.

A szabályozás egyfelől ugyan automatikus nyilvánosságkorlátozást jelent, aminek hiányában „minden egyes döntés-előkészítéssel kapcsolatos adat titkosításáról – a munkanyagok védelme és a döntéshozatali eljárás, illetve a szerv működésének hatékonysága érdekében – külön döntést kellene hozni”, ami „elviselhetetlen adminisztrációs terhet jelentene” az érintett szervek számára,¹⁵ de a formális, előzetes minősítési követelmény hiánya nem jelenti azt, hogy ne kellene alapos mérlegelést végeznie az adott szervnek. „Amennyiben az adatkezelő szerv a közérdekű adat kiadásának megtagadása mellett dönt, ezt [...] alkotmányos követelmények érvényesülése érdekében megfelelően indokolni köteles”, aminek „egyrészt ki kell terjednie arra, hogy pontosan milyen folyamatban lévő eljárásban meghozandó döntés megalapozását szolgálja a kiadni kívánt közérdekű adat, másrészt arra is, hogy a közérdekű adat kiadása mennyiben befolyásolja a szóban forgó döntés meghozatalát”.¹⁶

Az egyes közigazgatási eljárások során keletkezett iratok jelentős része nyilvánvalóan döntés megalapozását szolgáló adat, amelynek a nyilvánossága tehát a fentiek szerint korlátozott, tág teret engedve ugyanakkor az adatot kezelő szerv mérlegelésének. Érdemes azonban megnézni, hogy mennyiben állnak ezzel összhangban a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) szabályai.

A Ket. alapelvként vagy általános szabályként nem rendelkezik sem az egyes eljárások nyilvánosságáról, sem azok titkosságáról.¹⁷ Fogódzót így a védett adatok védelméről szóló 17. § (1) bekezdés és az iratbetekintést szabályozó 68. § adhat. Ezek szerint a közigazgatási eljárás során az ügyfélen és tanúkon kívül „harmadik személy akkor tekinthet be a személyes adatot vagy védett adatot tartalmazó iratba, ha igazolja, hogy az adat megismerése joga érvé-

14 E kitétel 2015. október 1-jével került be a jogszabályba, és az információszabadság jelentős korlátozását jelentheti, mivel elvileg szinte bármilyen adat alapja lehet egy később meghozandó döntésnek is. A szabály alkotmányossági aggályokat vet fel, a korábbi alkotmánybírósági gyakorlattal való összhang legfeljebb e kitétel igen szűk értelmezésével valósítható meg.

15 12/2004. (IV. 7.) AB-határozat

16 21/2013. (VII. 19.) AB-határozat

17 Bővebben: RIXER Ádám: *A köz természete. Új irányok a magyar közigazgatásban és a közigazgatás-tudományban*, Patrocínium, Budapest, 2013, 119.

nyesítéséhez, illetve jogszabályn vagy hatósági határozaton alapuló kötelezettsége teljesítéséhez szükséges, valamint ha a védett adat megismerésének törvényi feltételei fennállnak.”¹⁸ A korlátozás nem véletlenül szorítkozik a védett adatra, a törvényhez tartozó kommentár szerint „a jogszabályi megfogalmazás oka, hogy [ha] az iratok közt közérdekű, vagy közérdekből nyilvános adatok vannak, akkor abba az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény szabályai alapján bárki betekinthe.”¹⁹

A fenti szakaszok alapján tehát a személyes és védett adatokon kívül nincs korlátozva az iratbetekintés joga harmadik személyek (potenciálisan bárki) számára, amiből az következik, hogy ezen iratbetekintéseket az információszabadság szabályai (elsősorban a döntés megalapozását szolgáló szabályok) szerint kell megítélni. A Ket. 17. §-a alapján a személyes adatok és a védett adatok²⁰ esetén a hatóságnak kell gondoskodnia arról, hogy azok ne kerüljenek nyilvánosságra és ne juthassanak illetéktelen személyek tudomására. Megjegyzendő, hogy sok esetben a védett adat olyan adatokat jelent, amelyeknek titkossága az érintettek rendelkezésén is múlik (a természetes személy felhatalmazást adhat személyes adatainak akár nyilvánosságra hozatalára is, egy-egy dokumentum vagy információ kapcsán az érintett vállalkozás nyilatkozhat úgy, hogy az nem képezi üzleti titkát stb.), a hatóságnak ezeket figyelembe véve kell a 17. §-ban foglaltaknak eleget tennie.

2.3. A média jelenléte a hatósági ellenőrzéseken

Manapság teljesen hétköznapi, hogy az elektronikus média bekapcsolódik a közigazgatási hatóságok mindennapos jogalkalmazó tevékenységébe, és nem csak úgy, hogy adatokat, információkat kér, hanem úgy is, hogy „real time” figyeli, rögzíti és bemutatja az eseményeket.

A hírek között is előfordul olykor tudósítás a hatósági tevékenységről, de ilyenkor a hatóságok által rögzített felvételek kerülnek sugárzásra. Más a helyzet, ha a műsorkészítők „elkísérik” a hatóságot pl. a (helyszíni) ellenőrzésre, saját felvételeket készítenek, és ezeket bemutatják. A Hír TV Panaszkönyv című műsorának példának okáért a gerincét adja, hogy a műsorkészítők gyakran tartanak a Nemzeti Élelmiszerlánc-biztonsági Hatósággal „bevetésre” (pl. a közétkeztetés helyzetének ellenőrzése különféle településeken).

Kutatócsoportunk az alábbi kérdéseket tette fel fenti műsor szerkesztőségének elektronikus levélben:

- Mi az oka annak, hogy pl. a NÉBIH-et vagy más hatóságot rendszeresen elkísérik az ellenőrzésekre?

18 Ket. 68. § (3) bekezdés

19 Complex Jogtár: *Kommentár a Ket. 17.§-hoz.* A kommentár ugyanakkor tévesen és indokolatlanul le is szűkíti e szakasz értelmezését, amikor azt mondja, hogy „e jogszabályhely személyes adatokat tartalmazó iratokról beszél (illetve védett adatokról), azonban minden hatósági irat – főszabály szerint – szükségszerűen az ügy ügyfeleihez köthető, így személyes adatoknak tekinthetők.” Ügyfél ugyanis jogi személy is lehet, mely esetében a személyes adatok védelméről nincs szó, így ekkor csak a védett adatok jelentenek korlátozást.

20 További izgalmas kutatási kérdésként merülhet fel, hogy a kissé bizonytalan tartalmú „törvény által védett titok és a hivatás gyakorlásához kötött titok” (együtt védett adat) fogalma pontosan mit takar, és hogy e – a közérdekű adatok megismerését végső soron korlátozó – szabály kiállná-e az alkotmányosság próbáját.

- Ismerik-e a vonatkozó jogszabályi hátteret, ha igen, meg tudnának-e nevezni vonatkozó jogszabályt?
- Milyen aktivitást fejt ki a stáb az ilyen alkalmakkor (kérdez, megtekint, dokumentumokba betekint stb.)?

A műorszám felelős szerkesztője az alábbi választ adta fenti kérdéseinkre: „Sajnos (...) a műsor készítésének folyamatáról nem áll módunkban részleteket elárulni. A célunk minden esetben a fogyasztók tájékoztatása, illetve a fogyasztói tudatosság növelése, ennek egyik eszköze a hatóságokkal való együttműködés, a hatóságok munkájának bemutatása is.”

Természetesen nem a műorkészítés kulisszatitkaira voltunk kíváncsiak, sokkal inkább arra, vajon egy ilyen jellegű riport készítői, szerkesztői tisztában vannak-e tevékenységük jogi relevanciájával. A jogszabályi háttér feltárása ugyanis korántsem egyszerű.

A fogyasztóvédelemről szóló 1997. évi CLV. törvény nem ismeri a média szerepét a „fogyasztói tudatosság növelése” terén, nem rendelkezik arról sem, hogy „ennek egyik eszköze a hatóságokkal való együttműködés” lenne.

A fenti kérdésekkel megkerestük a Nemzeti Élelmiszerlánc-biztonsági Hivatal Sajtóosztályát is, amely – részletező – válaszában kifejtette:

1. A NÉBIH (a továbbiakban: Hivatal) ellenőrzéseiben történő részvételi és forgatási igény minden esetben a médiumoktól érkezik a Hivatalhoz. A televíziós stábok ellenőrzésen való részvétele a Hivatal számára is több előnyt hordoz magában: egyrészt a „közös munka” révén maximálisan biztosítható a korrekt tájékoztatás, másrészt – a vásárló, a fogyasztó „színfalak” mögé történő beengedésével – kiváló lehetőséget nyújt a hatósági munka átláthatóvá tételéhez, hiteles bemutatásához.
2. A forgatást megelőzően minden esetben felhívják a sajtó figyelmét a betartandó alapvető szabályokra. Ezek közül a legfontosabb, hogy kizárólag akkor forgathatnak a helyszínen, ha ahhoz az ellenőrzött fél hozzájárul. Az engedélyt az újságírónak/riporternek kell megkérnie, ezzel is biztosítva, hogy az ellenőrzött ügyfél ne érezhesse a hatóság oldaláról érkező „elvárásnak” a kérést.
3. Kapcsolódó jogszabályok a NÉBIH szerint:
 - a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény;
 - az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;
 - a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény;
 - a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény.
4. A forgatócsoportnak a helyszínen lehetősége van interjút (a NÉBIH részéről kizárólag a nyilatkozattételre jogosult vezetővel), valamint vágóképeket készíteni. A hivatalos dokumentumokba nem tekinthetnek bele, csupán magát az eljárást kísérhetik figyelemmel illesztés céljából, az ügyfél által adott hozzájárulás keretein belül.

Az élelmiszerláncról és hatósági felügyeletéről szóló 2008. évi XLVI. törvény – idevágó – 44. § (1) bekezdés d) pontja viszont egyértelműen kimondja, hogy az élelmiszerlánc-felügyeleti szerv helyszíni ellenőrzésre feljogosított köztisztviselője, valamint jelenlétében az

Európai Bizottság szakértője és az általa kijelölt szakértő jogosult kizárólag az ellenőrzés során az eljárása dokumentálására a helyszínen kép-, illetve hangfelvételt készíteni.

Általánosabb következtetések levonására segítségül hívhatók a Ket. rendelkezései, de témánk szempontjából kevés fogódzót találunk. Kiindulási pontunk az, hogy a közigazgatási hatóság az eljárása során köteles betartani és másokkal is betartatni a jogszabályok rendelkezéseit.²¹ Természetesen igaz ez a hatósági ellenőrzésekre is.

A Ket. alapelvei között nem szerepel a nyilvánosság, a szóbeliség, a közvetlenség, vagy a nyilvános tárgyalás elve.²² Minden bizonnyal azért sem, mert a közigazgatási eljárásban – elmentében a polgári vagy büntetőperes eljárásokkal – a legritkább esetben kerül sor tárgyalás tartására. Másrészt a közigazgatási eljárásban a nyilvánossághoz hagyományosan nem társítottak garanciális jelentőséget.²³ (Természetesen ez nem jelenti azt, hogy ne lehetne a nyilvánosság alapelvét a közigazgatási eljárásban is kodifikálni.)

A közigazgatási eljárásban a tárgyalás nyilvánosságának a követelményére találunk ugyan példát az Emberi Jogok Európai Bíróságának gyakorlatából,²⁴ a Ket. is utal az ügyféli beleegyezésen alapuló nyilvános tárgyalásra, valamint – közvetve – a közmeghallgatás nyilvánosságára,²⁵ de mindebből nem következik, hogy a közigazgatási eljárás, vagy annak egyes szakaszai (beleértve a hatósági ellenőrzést) – főszabályként – nyilvánosak („sajtónyilvánosak”) lennének. A Ket. sem a szemlére, sem a helyszíni ellenőrzésre nem rendeli el a tárgyalásra vagy a közmeghallgatásra vonatkozó szabályok megfelelő alkalmazását. A közérdekű adatok nyilvánosságára és az ezzel összhangban álló, iratbetekintésre vonatkozó szabályokból szintén nem következik a helyszíni ellenőrzés nyilvánossága: a sajtó esetleges jelenléte e cselekményeknél sem közérdekűadat-igénylésnek, sem iratbetekintésnek nem minősül – az adott cselekményen való egyidejű jelenlét során azzal kapcsolatban még sem (közérdekű) adat,²⁶ sem irat nem létezik. Ezek alapján kijelenthető, hogy a közigazgatási eljárásban, annak egyes szakaszaiban, az eljárási cselekményeknél azok lehetnek jelen, akik az ügyben – jogszabály rendelkezésénél fogva – érintettek: pl. ügyfél, szakértő, tanú.

Nyilvánvalóan a televíziós csoport – ténylegesen – úgy vehet részt közigazgatási hatósági eljárásban, hatósági ellenőrzésen, ha ahhoz a közigazgatási hatóság hozzájárult. Kérdéses azonban, hogy van-e hatásköre (jogi lehetősége) a közigazgatási hatóságnak ilyen típusú hozzájárulást adni. A fenti szabályok alapján úgy tűnik, hogy nincs. Ez ráadásul olyan eljárási döntés lenne, amelyről a hatóságnak végzésben kellene határoznia.

Ehhez kapcsolódik annak a kérdésnek a megválaszolása is, hogy vajon az ügyfél hozzájárulhat-e ahhoz, hogy idegen forgatócsoport felvételeket készítsen lakhelyén, székhelyén vagy telephelyén, amíg a hatósági ellenőrzés tart. A válasz részben spekulatív: az ügyfél be-

21 Ket. 1. § (1) bekezdés

22 Vö. Pp. 5. § (1) bekezdés

23 Vö. szerk. BARABÁS Gergely, BARANYI Bertold, KOVÁCS András György, ASZALÓS Dániel: *Nagykommentár a közigazgatási eljárási törvényhez*, Wolters Kluwer, Budapest, 2013, 481.

24 Lásd C. 8790/79. Sramek v. Austria; C. 29447/95 Eisenstecken v. Austria

25 Ket. 62. § (4) bekezdés, és Ket. 63. § (1) bekezdés c) pont

26 Bár az adat fogalmát az Infotv. nem határozza meg, a közérdekű adatnak fogalmi eleme a „bármilyen módon vagy formában rögzítettség”.

leegyezhet ugyan, hogy felvételek készüljenek róla vagy ingatlanáról harmadik személy által az ellenőrzés alkalmával, de ez a beleegyezés nem pótolja, nem pótolhatja a hatóság hiányzó hatósági jogkörét harmadik személy bevonására.

A sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény (Smtv.) 4. § (3) bekezdése értelmében a sajtószabadság gyakorlása nem valósíthat meg bűncselekményt vagy bűncselekmény elkövetésére való felhívást, nem sértheti a közérkölcset, valamint nem járhat mások személyiségi jogainak sérelmével. A Smtv. 16. szakasza pedig kimondja, hogy a médiatartalom nem sértheti az alkotmányos rendet. Mindezek alapján megállapítható az is, hogy a médiának, a sajtónak a tájékoztatáshoz való joga nem magasabb rendű a közigazgatás törvényességének követelményénél, beleértve a közigazgatási eljárás törvényességét.

A sajtó a tájékoztatás során nem valósíthat meg jogsértést, de nem irányulhat a demokratikus alapértékek tagadására, elutasítására sem.²⁷ Megállapítható ugyanakkor, hogy az Smtv. – korlátozó – rendelkezéseit nem sérti, ha forgatócsoport tart a hatósággal a helyszíni ellenőrzésre, az Smtv. rendszerébe az ilyen tájékoztatási tevékenység és médiatartalom beilleszthető. A Ket. és a többi hivatkozott jogszabály a média ilyen típusú részvételét a hatósági eljárásban ugyan kifejezetten nem tiltja, de a tilalomra a közigazgatási eljárásjog rendszeréből következtethetünk. Ha a média részt vehet a hatósági ellenőrzésen, akkor ez a jog olyan másik harmadik személyt is meg kell hogy illessen, akinek ez érdekében áll (pl. a fogyasztókat kívánja védeni). Ebből viszont az is következne, hogy a jogos érdek szükséges és elégséges az ügyfélé váláshoz, az egyszerű érdek pedig ahhoz, hogy megfigyelői joga legyen az eljárásban. Ez a következtetés idegen a Ket. jelenlegi rendszerétől.

Álláspontunk szerint a hiányzó jogi szabályozás jogbizonytalanságot okoz, és feltétlenül szükséges lenne e kérdéskör tételes jogi szabályozása, akár az iratbetekintéssel kapcsolatos szabályok, akár a bírósági eljárások nyilvánosságáról szóló szabályok – megfelelő módosításokkal történő – alapulvételével.

3. A MÉDIA HATÓSÁGI FELÜGYELETE

3.1. Bevezető gondolatok

A közigazgatás tárgya az államilag szervezett társadalom, amelynek kulcsfontosságú eleme a média, azaz minden társadalmilag létrejött kommunikációs struktúra és e struktúrák hordozói. A média és a közigazgatás közötti kapcsolat tehát szükségszerű, az állam ugyanis a média tevékenységét elsődlegesen a közigazgatási szerveken keresztül kontrollálja. Azt a médiát, amelynek pedig jelentős szerepe van az állami működés ellenőrzésében.

Elvileg ugyan a médiahatóság által ellátott feladatok jelentős részét más hatóságokhoz, adott esetben hatósági jogkör nélkül működő állami szervhez (médiabudszman), illetve

27 szerk. KOLTAY András, LAPSÁNSZKY András: *Médiaügyi kommentárok*, Wolters Kluwer, Budapest, 2014, 87.

önszabályozó szervezethez lehetne telepíteni,²⁸ a nemzetközi tendenciák alapján²⁹ jellemzően mégis önálló vagy a hírközlési hatóságokkal közös (konvergens) hatóságok látják el a médiát érintő tartalmi előírások feletti felügyeletet. A magyar médiahatóságot, a Nemzeti Média- és Hírközlési Hatóságot (NMHH), illetve annak Médiatanácsát az új magyar médiaszabályozás keretében elfogadott törvények közül a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény (Mttv.) intézményesítette.

3.2. A nemzeti média- és hírközlési hatóság jogállása

A Nemzeti Média- és Hírközlési Hatóság az Mttv. által meghatározott normák alapján látja el tevékenységét. Jogállását az Mttv. 109. § (1) bekezdése mellett a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény (Ksztv.) 1. § (2) bekezdés i) pontja határozza meg.

A Ksztv. alapján az NMHH önálló szabályozó szervnek minősül. Az állami szervek eme új kategóriáját az Alaptörvény 23. cikke³⁰ hozta létre. A kiemelt szabályozás indokaként megjegyezhető, hogy az önálló szabályozó szervezetnek közérdek-érvényesítő szerepet (is) szán a jogalkotó az állami szervek között. Az Alaptörvény szóhasználatában a szabályozás inkább jogszabály-alkotási hatáskört takar, az önállóság pedig arra mutat rá, hogy a szerv nem áll a Kormány irányítása alatt.

Az NMHH vezetőjét a miniszterelnök nevezi ki 9 évre. E törvényi szabályozással összefüggésben említhető mega Velencei Bizottságvéleménye, miszerintily módon nem biztosítható a hatóság politikai függetlensége, ezért a bizottság módosítaná az elnök kinevezését a hatalomkoncentráció csökkentése és a személyi politikai semlegességének biztosítása érdekében.³¹ A Velencei Bizottság előbbi aggályait az NMHH hivatali szervezetén belüli, de önálló jogi személyiséggel bíró és autonóm hatósággal, a Médiatanáccsal szemben is fenntartja, amelynek elnöki pozícióját szintén az NMHH elnöke tölti be. A Médiatanács öt tagját – jogelődje, az ORTT tagjaihoz hasonlóan – az Országgyűlés választja meg, viszont míg a rádiózásról és televíziózásról szóló 1996. évi I. törvény (Rttv.) 33. § (1) bekezdés c) pontja alapján a képviselőcsoportok egyenként jelöltek egy-egy tagot a testületbe, addig az Mttv. alapján a képviselőcsoportok egy-egy tagjából álló eseti bizottság tesz javaslatot a négy tagra.³² Ez a megoldás sokkal nagyobb kompromisszumkényszerrel telepít a képviselőcso-

28 Mérték Médiaelemző Műhely: *A médiafelügyeleti feladatok ellátása*, 2003. Forrás: www.cij.hu/hu/wp-content/uploads/2013/10/hatosag_vitaanyag_final.pdf (2015. 07. 29.)

29 Példánk okáért: Franciaországban Conseil Supérieure de l'Audiovisuel, Egyesült Királyságban: Ofcom

30 „Az Országgyűlés sarkalatos törvényben a végrehajtó hatalom körébe tartozó egyes feladat- és hatáskörök ellátására és gyakorlására önálló szabályozó szervezetet hozhat létre.”

31 CDL-AD (2015) 015-e Opinion on Media Legislation (ACT CLXXXV on Media Services and on the Mass Media, Act CIV on the Freedom of the Press, and the Legislation on of Advertisement Revenues of Mass Media) of Hungary, adopted by the Venice Commission at its 103rd Plenary Session (Venice, 19–20 June 2015) 59–61 points.

32 Mttv. 124. § (3) és (4) bekezdések

portokra, ugyanakkor kétségekívül nem biztosítja azt, hogy minden képviselőcsoport jelölje részt vehessen a Médiatanácsban.³³

Indokolt e helyütt idézni az Alkotmánybíróság 46/2007. (VI. 27.) határozatát, amelynek tárgya az ORTT tagjainak megválasztása, és amely a Médiatanács tagjai vonatkozásában is helytálló lehet: „A Médiatörvény 31. § (2) bekezdése szerint az ORTT tagjai is csak a törvénynek vannak alárendelve, és tevékenységük körében nem utasíthatók. Az önálló és befolyásmentes működést biztosítja, hogy a tagok mandátuma szabad, nem hívhatók vissza. A politikai és gazdasági összeférhetetlenségre vonatkozó szabályok a függetlenség további garanciái. Az Országgyűlés által megválasztott ORTT-tagok mandátuma elvlik a törvényhozási ciklustól. [...] Ezek a törvényi rendelkezések elvileg képesek biztosítani az ORTT-tagok függetlenségét, és kizárják, hogy a parlamenti pártok formálisan érvényesíthessék befolyásukat.” „[A]z a tény, hogy a parlamenti képviselők szavaznak az ORTT tagjairól, biztosítja, hogy a személyekről való döntés demokratikus eljárás eredménye.” A Médiatanács megválasztásának szabályozása elvileg eleget tesz az alkotmányosság kívánalmainak: tagjait az Országgyűlés választja, és nem a kormánypártok számára mindenkor rendelkezésre álló egyszerű többséggel, hanem a megegyezés kényszerét az ellenzéki pártok irányába is kiterjesztő minősített, kétharmados többséggel.³⁴ A törvényben előírt kétharmados többség ugyan általában arányos összetételt biztosít, ám ez az arányosság sérül akkor, ha a kormánypárt egyedül birtokolja a parlamenti helyek több mint kétharmadát.

Az önálló szabályozó szervek, miként az elnevezés is mutatja, nemcsak jogalkalmazó, hatósági tevékenységet végeznek, hanem normaalkotásra is jogosultak, vagyis jogalkotási jogkörrel rendelkeznek. Az Alaptörvény rendeletalkotási jogosultsággal ruházta fel tehát az NMHH vezetőjét, míg e hatáskörrel a jogelőd szervek (Nemzeti Hírközlési Hatóság, Országos Rádió és Televízió Hatóság) nem rendelkeztek – ez egyértelműen a jogutód szerv jogállásának erősödését eredményezi. Az NMHH közel öt éves működése során több tucat rendelet került kiadásra.

3.3. A Nemzeti Média- és Hírközlési Hatóság médiafelügyeleti hatósági tevékenysége

Az NMHH önálló hatáskörrel rendelkező szervei a Médiatanács és Hivatal az Mttv. IV. fejezete szerinti eljárásokban, az Mttv. 144. § (1) bekezdése szerint hatóságként hatósági felügyeleti jogkört gyakorolnak, amelynek során a Ket. szabályait alkalmazzák az Mttv.-ben foglalt eltérésekkel, azaz a médiafelügyeleti eljárás privilegizált eljárásnak minősül a Ket. általános és különös eljárási szabályainak viszonyában.

Míg a korábbi szabályozás alapján nem minden esetben volt egyértelműen elkülöníthető az ORTT közhatalmi és polgári jogi feladatellátása (ahogy erre az Alkotmánybíróság többször is utalt),³⁵ az Mttv. e tekintetben világos, átlátható és kiszámítható jogalkalmazási rend-

33 KOLTAY András, LAPSÁNSZKY András: *Az új magyar médiaszabályozás alkotmányossági kérdései*, Iustum Aequum Salutare, 2011/2, 89.

34 *Uo.*, 89.

35 Ld. 57/2009. (V. 20.) és 46/2007. (VI. 27.) AB-határozatokat

szert alakított ki, amely megvalósítja és érvényesíti a közigazgatás törvény alá rendeltségének európai és alkotmányossági követelményét.³⁶

A törvény 182. §-ában sorolja fel a Médiatanács hatósági jogkörbe tartozó feladatait, ezek többek között a következők:

- ellátja az általa kötött hatósági szerződések általános hatósági felügyeletét,
- hatósági felügyeletet gyakorol például a gyermekek és a kiskorúak védelmére vonatkozó előírások, a műsorkvótákra vonatkozó követelmények tekintetében,
- gyakorolja a más tagállamban letelepedett médiatartalom-szolgáltatók által elkövetett jogsértésekkel kapcsolatos hatósági hatásköröket,
- megállapítja a médiaszolgáltatási alapidíjat,
- médiapiaci ágazati vizsgálatot folytat le,
- piacfelügyeleti eljárást folytat le,
- szakhatósági feladatokat lát el.

A Médiatanács gyakorolja a kiemelt hatósági hatásköröket, azonban bizonyos területeken a Hivatalnak is van hatósági hatásköre (például vezeti a hatósági nyilvántartásokat, elbírálja a kiegyensúlyozott tájékoztatás kötelezettségének megsértése miatt tett kérelmeket nem jelentős befolyásoló erejű, illetve nem közszolgálati médiaszolgáltatók esetén, felügyeli a közszolgálati és közösségi médiaszolgáltatásban közzétett reklámra és közérdekű közleményre vonatkozó, valamint a hallási fogyatékkal élők számára hozzáférhető műsorszámokra vonatkozó szabályok érvényesülését stb.).

A Médiatanács eljárása során a tényállás tisztázása érdekében jogosult akár az üzleti titkot tartalmazó eszközt, dokumentumot is megvizsgálni, illetőleg az ügyfelet, az eljárás egyéb résztvevőjét, valamint különösen indokolt esetben az említetteken kívül más személyt vagy szervezetet is adatszolgáltatásra, bizonyos eszközök átadására kötelezni.³⁷ Ez a médiatörvény egyik legvitatottabb passzusa. Egyes vélemények alapján e rendelkezés a sajtószabadság durva és szükségtelen korlátozása, amely lehetővé teszi a hatóság számára az önkényes jogalkalmazást és a korlátlan adatszolgáltatás előírását, míg mások vélekedése szerint megfelelő garanciális biztosítékokat tartalmaz a törvény, ugyanis a hatóság kizárólag a törvény által meghatározott hatáskörébe tartozó hatósági ügyben indított hatósági eljárásban, a tényállás tisztázása érdekében (tehát az egyedi, konkrét ügy jogilag releváns tényeinek feltárása érdekében) jogosult adatszolgáltatás előírására.³⁸

3.4. A Nemzeti Média- és Hírközlési Hatóság szerepe a fogyasztóvédelemben

A fentiekben túl érdemes kitérni arra a – magyar jogirodalomban eddig nemigen tárgyalt – kérdésre, hogy milyen szerepe lehet az NMHH-nak a fogyasztók védelmében.

³⁶ KOLTAY-LAPSÁNSZKY: *i. m.*, 94.

³⁷ Mttv. 155. § (2), (3), (9) bekezdések

³⁸ Vö. MAJTÉNYI László, POLYÁK Gábor: *A szabadság hazai hagyományának megtagadása*, *Közjogi Szemle*, 2011/1, 10. és KOLTAY-LAPSÁNSZKY: *i. m.*, 102.

A fogyasztóvédelem kialakulása és fejlődése szoros kapcsolatban áll a gazdasági viszonyokkal is, mivel a piaci viszonyok közepette – a fogyasztók hátrányára – képes megbomlani a gazdasági élet szereplői közötti egyensúly. A fogyasztó – többek között a piaci módszerek ismeretének hiánya miatt – kiszolgáltatott helyzetbe kerülhet a kereskedőkkel, szolgáltatókkal, vállalkozásokkal szemben, ennek pedig egyik legérzékenyebb területe az elektronikus reklám, ahol különösen felértékelődik az állam fogyasztóvédelmi tevékenysége és ezáltal a fogyasztók (nézők) jogainak hatékony védelme. Ez a felismerés alapozta meg a fogyasztóvédelem – mint a magánjogi jogviszonyokba történő állami beavatkozás – intézményesítését a médiajog területén is.³⁹

A fogyasztóvédelem állami intézményrendszerében kiemelkedő szerepet töltenek be a fogyasztóvédelmi hatóságok, így a Nemzeti Fogyasztóvédelmi Hatóság, a Magyar Nemzeti Bank, a Gazdasági Versenyhivatal, valamint más, jogszabály által feljogosított ún. speciális fogyasztóvédelmi hatóságok.⁴⁰ A Nemzeti Fogyasztóvédelmi Hatóság általános hatáskörű szerv, ez azonban nem érinti a más jogszabályban egyéb szervek számára biztosított fogyasztóvédelmi feladat- és hatásköröket. Ebből kiolvasható, hogy a médiaszolgáltatók által közvetített reklámok esetén bekövetkező fogyasztói jog- és érdeksérelmek orvoslása – mint speciális hatáskörű fogyasztóvédelmi hatóság – a Nemzeti Média- és Hírközlési Hatóság kompetenciájába tartozik. Mindezekre tekintettel fontosnak tartjuk a média és a fogyasztóvédelem témakörének áttekintését ebben a vonatkozásban.

Először az a kérdés vár tisztázásra, hogy vajon értelmezhető-e a klasszikus állami fogyasztóvédelmi tevékenység a mediaszolgáltatók által közvetített reklámok és a nézők közötti relációban? Ebben a tekintetben az Mttv. hallgat, viszont a fogyasztóvédelemről szóló 1997. évi CLV. törvény (Fgytv.) alapján el lehet indulni. Az Fgytv. 2. §-ában foglalt értelmező rendelkezés szerint fogyasztó az az önálló foglalkozásán és gazdasági tevékenységi körén kívül eső célok érdekében eljáró természetes személy, továbbá a békéltető testületre vonatkozó szabályok alkalmazásában az önálló foglalkozásán és gazdasági tevékenységi körén kívül eső célok érdekében eljáró, külön törvény szerinti civil szervezet, egyházi jogi személy, társasház, lakásszövetkezet, mikro-, kis- és középvállalkozás is, aki, illetve amely árut vesz, rendel, kap, használ, igénybe vesz vagy az áruval kapcsolatos kereskedelmi kommunikáció, ajánlat címzettje. A citált fogalom meghatározás egyértelművé teszi, hogy „az áruval kapcsolatos kereskedelmi kommunikáció címzettje” fogyasztónak tekinthető, így indokolt a média és a fogyasztóvédelem összefüggéseinek vizsgálata.

Az NMHH fogyasztóvédelmi tevékenységére két alkalommal tesz – implicit utalást – az Mttv., egyszer a piacfelügyeleti tevékenységet intézményesítő 168. §-ban, másodszor az NMHH hatósági hatáskörét körülíró 182. §-ban.

39 Ezzel összefüggésben lásd többek között Viktor Luszcz: *Fogyasztóvédelem az Unióban*, Cég és Jog, 2002/5, 41–47.

40 Ebbe a körbe sorolható egyebek mellett a Nemzeti Közlekedési Hatóság, a Magyar Élelmiszerbiztonsági Hivatal, a Magyar Kereskedelmi és Engedélyezési Hivatal, a Magyar Bányászati Hivatal, az Országos Mérésügyi Hivatal, az Országos Tisztifőorvosi Hivatal, a Nemzeti Média- és Hírközlési Hatóság, valamint az Egenlő Bánásmód Hatóság.

3.4.1. Fogyasztóvédelem a piacfelügyeleti tevékenység keretében

A piacfelügyelettel összefüggésben a törvény rendelkezése szerint a Médiatanács – hatáskörének terjedelmében – a médiapiac zavartalan, eredményes, sokszínű működésének, a műsorterjesztést és a médiaszolgáltatást végzők, sajtóterméket kiadók, a nézők, hallgatók, olvasók, előfizetők és felhasználók érdekei védelme, valamint a nemzeti kultúra és a vélemények sokszínűségének megőrzése érdekében, a tisztességes és hatékony piaci verseny fenntartásának elősegítése, a piaci folyamatok megismerése és a médiapolitikai szempontok, illetve az e törvényben meghatározott egyéb célok átfogó értékelése, elemzése és hatósági felügyelete céljából piacfelügyeleti tevékenységet végez.⁴¹ A kissé bonyolult sikeredett törvényhely egyértelművé teszi, hogy – egyebek mellett – a „nézők, hallgatók, olvasók, előfizetők és felhasználók érdekei[nek] védelme” teszi indokolttá a médiapiac hatósági felügyeletét.

A piacfelügyeleti tevékenység eredményét tekintve kiemelhető, hogy a Médiatanács egyrészt értékeli az eljárás tárgyát képező szolgáltatásokkal, tevékenységekkel összefüggő jogérvényesülést, jogsértés hiányában pedig szükség szerint kötelezettségeket állapíthat meg és azok teljesítésének feltételeit is meghatározhatja. Az eljárás eredményét tekintve kiemelhető másrészt az is, miszerint meghatározza a jogsértések megelőzésével, az önkéntes jogérvényesülés előmozdításával, a piaci folyamatok zavartalan működésével kapcsolatos állami beavatkozás irányait, módszerét, fejlesztésének, esetleges átalakításának szempontjait, médiapolitikai következtetéseit.⁴²

3.4.2. Fogyasztóvédelem az NMHH hatósági hatáskörei között

A nézők, vásárlók, előfizetők és felhasználók (a korábbiaknak megfelelően együttesen: fogyasztók) érdekeinek érvényesítése megjelenik az NMHH hatósági hatáskörei között is. A törvény 182. § (1) bekezdése ugyanis akként rendelkezik, hogy a Médiatanács – egyebek mellett – hatósági hatásköreiben egyrészt ellátja az általa kötött hatósági szerződések általános hatósági felügyeletét; másrészt hatósági felügyeletet gyakorol többek között a gyermekek és a kiskorúak védelmére vonatkozó előírások, a kereskedelmi közleményekre vonatkozó előírások, a termékmegjelenítésre vonatkozó rendelkezések, a reklámra és televíziós vásárlásra vonatkozó kötelezettségek teljesítése fölött.

Kiemelendő az is, hogy az NMHH hatósági jogkörei között megtalálható fogyasztóvédelmi jellegű kompetenciák meghatároznak egyfajta erősrendet a hatóság által felügyelendő jogintézmények közül, ezzel preferenciát írva elő a hatósági tevékenység számára. Ennek megfelelően a gyermek- és fiatalkorúak érdekeinek védelme, a termékmegjelenítésre, a televíziós vásárlásra, vagy éppen a kereskedelmi reklámok tartalmára vonatkozó rendelkezések feletti jogszerepségi szempontú kontroll jelenti a médiahatóság hatósági fellépésének „főcsapását”.

Az idézett rendelkezések ugyanakkor azt is egyértelművé teszik, hogy a jogalkotó nem csupán anyagi oldalról közelítve szabályozza (tipikusan tilalmak formájában) a kereskedelmi reklámok tartalmával kapcsolatos követelményeket, hanem azok megsértése esetén hatósági jog-

⁴¹ Mttv. 168. § (1) bekezdés

⁴² Mttv. 168. § (6) bekezdés

kört telepít a Médiatanácshoz, önálló szerkezeti egységben szól továbbá az eljárás eredményeképpen alkalmazható jogkövetkezményekről. A jogsértés megállapítása esetén a Médiatanács vagy a Hivatal jogkövetkezményt alkalmazhat. A magyar médiajogi szabályozás a törvényben előírt kötelezettségek megsértését az Mttv. 186. és azt követő szakaszaiban megfogalmazott közigazgatási szankcióknak rendeli alá, amelyek alapján a Médiatanács (1) a jogsértőt meghatározott időre kizárhatja a Médiaszolgáltatás-támogató Vagyonkezelő Alap pályázatainak való részvétel lehetőségéből, (2) bírságot szabhat ki a jogsértővel szemben, (3) a jogsértőt kötelezheti közleménynek vagy a határozatnak a jogsértő internetes honlapjának nyitóoldalán, sajtótermékben vagy megjelölt műsorszámban történő közzétételére, (4) meghatározott időtartamra felfüggesztheti a médiaszolgáltatási jogosultság gyakorlását, (5) törölheti azon médiaszolgáltatást a nyilvántartásból, amelyben a jogsértést elkövették, illetve (6) azonnali hatállyal felmondhatja a médiaszolgáltatási jogosultság tárgyában megkötött hatósági szerződést.⁴³

Az Mttv. 185. § (2) bekezdése szerint a jogkövetkezmény alkalmazása során a Médiatanács és a Hivatal az egyenlő bánásmód elvét követve a fokozatosság és az arányosság elvére tekintettel jár el; a jogsértés súlyához, illetve ismétlődéséhez igazodóan alkalmazza a fokozatosság elvét, valamint az eset összes körülményéhez és a jogkövetkezmény által elérni kívánt célhoz képest arányos jogkövetkezményt alkalmaz. A hatóság tehát a jogalkalmazás körében jogosult a mérlegelésre (pl. felfüggesztés időtartama, bírság összegének meghatározása), a mérlegelési jogkör korlátjaként jelen van azonban a regulációban a fokozatosság és az arányosság elve. E szankciókra vonatkozó szabályozás szintén éles kritikák tárgya. Vannak, akik azt kifogásolják, hogy a jogkövetkezmények a lineáris és nem lineáris médiaszolgáltatások esetében közvetlenül, a sajtótermékek esetében a magas bírságokon keresztül közvetve az adott médium megszűnéséhez vezethetnek, továbbá nincsenek megfelelően kidolgozva az arányosság és fokozatosság részletszabályai. Ez a túlzott szigorúság és a törvényi hiányosságok pedig a vélemény- és sajtószabadság aránytalan korlátozását jelentik.⁴⁴

4. ÖSSZEGRÉS

Tanulmányunkban a közigazgatás és média főbb kapcsolódási pontjaira tértünk ki, két jelentős aspektust: a média (és általában a nyilvánosság) közigazgatás működése feletti kontrollját, valamint a közigazgatás média működése feletti kontrollját vizsgálva.

A közigazgatás nyilvánossága kapcsán arra jutottunk, hogy különbséget kell tenni a közigazgatás (egészének) nyilvánossága és átláthatósága, illetve az egyes közigazgatási (hatósági) eljárások nyilvánossága között, valamint a (közérdekű) adatok és iratok megismerhetősége, illetve az egyes eljárási cselekmények nyilvánossága és a média azon való egyidejű jelenléte között. Míg a közérdekű adatok igénylésével és az iratbetekintéssel kapcsolatos szabályok nagyjából koherensek, addig a másik terület lényegében szabályozatlan, ami jogbizonytalanságot, a nyilvánosság érvényesülése szempontjából hasznos, de a Ket. szabályozási logikájával összhangban nem álló tényleges gyakorlatot eredményez.

⁴³ Mttv. 187. § (3) bekezdés

⁴⁴ MAJTÉNYI-POLYÁK: *i. m.*, 8.

A média hatósági felügyelete során pedig azt kell kiemelni, hogy a jogalkotónak e terület szabályozásakor különös körültekintéssel kell(ene) eljárnia, fokozottan figyelembe véve a média alkotmányos szerepét és kontrollfunkcióját is.⁴⁵ Egyetértünk azzal, hogy a szabályozás kialakítása során arra kell törekedni, hogy a médiarendszert alakító döntések is objektív, mérlegelést nem igénylő szempontok alapján szülessenek.⁴⁶ A jelenlegi szabályozás több területen (pl. a fogyasztók érdekeinek védelme) eredményesen és hatékonyan működik ugyan, de más, épp a kontrollfunkció szempontjából alapvető kérdéseket illetően – függetlenség kérdése, szankciók szigora és alkalmazási köre – jelentős aggályok merülnek fel.



SUMMARY IN ENGLISH: The relationship between public administration and media can be interpreted from two viewpoints. The first one focuses on the control of the state by the media (and by society). The transparency of public administration and governance is both a cornerstone of any democratic state and also an important pillar of modern electronic public services. However, it is important to define the limits of transparency and to distinguish between the transparency of the operation of the public administration as a whole and the transparency of a single procedure. The other aspect, expounded in the second part of this essay, focuses on the issue of how the state controls media by its regulatory authority, and whether the regulatory system takes into account the constitutional (control) function of the media.

Dr. Bencsik András, PhD (bencsik.andras@ajk.pte.hu): adjunktus, a Pécsi Tudományegyetem Állam- és Jogtudományi Kar Közigazgatási Jogi Tanszékének oktatója. Oktatási tevékenysége a közigazgatás szervezeti és intézményrendszerének, valamint a közigazgatás működésének valamennyi területére kiterjed. Kutatási területei közé tartoznak különösen a közigazgatási hatósági eljárás, a közigazgatási bíráskodás, a közigazgatási működés törvényességének biztosítása, valamint a gazdasági közigazgatás (versenyjog, fogyasztóvédelem) témakörei. E tárgykörökben több pályázati kutatási és szakértői projektben vett részt kutatóként. Számos hazai és külföldi (angol nyelvű) publikáció szerzője. 2015-ben jelent meg „A közigazgatás törvényességétől a technológiai innovációig” című monográfiája. Doktori értekezését 2013-ban védte meg „A fogyasztói jogok tartalmának és érvényesülésének közjogi keretei Magyarországon” címmel, a vonatkozó kutatásait összefoglaló könyve 2016-ban jelenik meg a Dialóg Campus Kiadó gondozásában „A fogyasztóvédelem közjogi keretei” címmel. 2015 januárja óta az általános közigazgatási rendtartásról szóló törvényt előkészítő

45 Érdemes itt utalni például az Alkotmánybíróság 165/2011. (XII. 20.) számú határozatára, amely a Média- és Hírközlési Biztos akkor hatályos szabályozásának alkotmányellenességét mondta ki, mivel nincs alkotmányos indoka annak, hogy a Biztos – pontosabban meg nem határozott – „méltányolandó érdekek” sérelme vagy annak veszélye esetén – akár a szerkesztői szabadságot közvetlenül is érintve – fellépjen.

46 Mérték Médiaelemző Műhely: *A médiafelügyeleti feladatok ellátása*, 2003, 1. Forrás: www.cij.hu/hu/wp-content/uploads/2013/10/hatosag_vitaanyag_final.pdf (2015. 07. 29.)

Kodifikációs Bizottság tagja. Tagja a Public Governance, Administration and Finances Law Review bíráló bizottságának. Az MTA köztestületi tagja.

Dr. habil. Fábián Adrián (fabian.adrian@ajk.pte.hu): dékánhelyettes, tanszékvezető egyetemi docens, PTE ÁJK Közigazgatási Jogi Tanszék. 2002-től oktat a Pécsi Tudományegyetem Állam- és Jogtudományi Karán közigazgatási jogi tárgyakat. Hat könyve és több mint száz írása jelent meg. Főbb kutatási területei: közigazgatás-elméleti kérdések, közigazgatás szervezeti rendszere, hivatásos közzolgálat. Tagja a Magyar Tudományos Akadémia (MTA) IX. Gazdaság- és Jogtudományok Osztálya keretei között működő Közigazgatástudományi Albizottságnak. A *Studia Iuridica Auctoritate Universitatis Pécs Publicata*. *Essays of Faculty of Law University of Pécs*. *Yearbook of [year]* angol nyelvű évkönyv, valamint a *Public Governance, Administration and Finances Law Review* szerkesztőbizottságának tagja. Az MTA köztestületi tagja. 2013. szeptember 30-án az Országgyűlés a Nemzeti Választási Bizottság tagjává választotta. Németül és angolul beszél.

Dr. Pál Emese (pal.emese@ajk.pte.hu): 2014-ben végzett a Pécsi Tudományegyetem Állam- és Jogtudományi Karán *summa cum laude* minősítéssel, majd ugyanebben az évben kezdte meg a munkát a Közigazgatási Jogi Tanszéken, mint nappali tagozatos PhD-hallgató. A 2008–2009-es tanévet a Toulouse-i Egyetem jogi karán töltötte. 2013-ban egy tanéven keresztül a PTE ÁJK-n újjászerveződő Óriás Nándor Szakkollégium alelnöke. Az Országos Tudományos Diákköri Konferencia Jogi Szekciójában „A helyi önkormányzatok feletti törvényességi kontroll változásai” című pályamunkája díjazásban részesült. Doktori értekezésének választott témája „a törvényesség elvének intézményi biztosítékai a választás kampány során” elnevezést viseli. Tudományos érdeklődése emellett kiterjed a közigazgatási bíráskodás, a közigazgatás-elmélet, továbbá a helyi önkormányzatok területére. Franciául és angolul beszél.

Dr. Szóke Gergely László, PhD (szoke.gergely@ajk.pte.hu): adjunktus, a Pécsi Tudományegyetem Állam- és Jogtudományi Kar Közigazgatási Jogi Tanszék Informatikai és Kommunikációs Jogi Csoport oktatója. Oktatási tevékenysége az informatikai jog és médiajog valamennyi területére kiterjed. Kutatási területei közé tartoznak különösen a személyes adatok védelme, a közérdekű adatok nyilvánossága és a közadatok újrahasznosítása, illetve az elektronikus eljárások szabályozása. E témakörökben több pályázati kutatási és szakértői projektben vett részt kutatóként vagy kutatásvezetőként. Számos hazai és külföldi (angol nyelvű) publikáció szerzője. Doktori kutatásait összefoglaló könyve 2015-ben jelent meg a HVG-ORAC gondozásában „Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén” címmel. 2007 óta a Pécsi Tudományegyetem belső adatvédelmi felelőse. 2010–2011 között adatvédelmi szakértőként dolgozott az Országgyűlési Biztos Hivatala Adatvédelmi Biztos Irodáján. Az *Infokommunikáció és jog* című szakmai folyóirat szerkesztője, valamint a *Studia Iuridica Auctoritate Universitatis Pécs Publicata*. *Essays of Faculty of Law University of Pécs*. *Yearbook of [year]* angol nyelvű évkönyv főszerkesztője.

A FELHŐALAPÚ SZÁMÍTÁSTECHNIKA HASZNÁLATA A KÖZ- ÉS ÜZLETI SZFÉRÁBAN

A felhőalapú számítástechnika lényege, hogy a felhasználónak nem szükséges komoly, szervezeten belüli informatikai infrastruktúrával rendelkeznie. Az ilyen, az internetről érkező szolgáltatásoknak persze több más szempont alapján is csoportosítható jellemzője lehet. A köz- és üzleti szféra számára költségcsökkentést, adatvédelmet, hatékonyságnövekedést és szervezeti-kultúra-változást, versenyképesség-növekedést jelent. A technológia elterjedését hátráltató tényezők technikai és humán eredetűek lehetnek. A felhőalapú technológia használatának gyakorisága az Európai Unióban országonként és méretkategóriánként eltérő az üzleti szférában. A magyar közszférában számos új szolgáltatás érhető el napjainkban.

KULCSSZAVAK:

felhőalapú számítástechnika, IaaS, PaaS, SaaS, magánfelhő, nyilvános felhő, közszféra, üzleti szféra



1. BEVEZETÉS

A technológiai változások közül különösen a mobil- és a felhőalapú számítástechnika, a Big Data, valamint a közösségi média produkálják az utóbbi években az információs technológiai (IT) szektor legnagyobb növekedését, létrehozva egy olyan információra és innovációra épülő „digitális világot”, amely lényeges kihívások elé állítja a köz- és az üzleti szférát. E technológiai újítások részben egymásra épülnek, összefonódnak. Éppen ennek köszönhető, hogy a felhőalapú számítástechnika kiemelkedik a fenti területek közül, ugyanis az mind önmagában (külön szolgáltatásként), mind pedig a többi egyre inkább elválaszthatatlan összetevőjeként is megjelenik.¹

A felhőalapú adatforgalom 2011-hez képest öt év alatt a hatszorosára nő, miközben az adatközpontokon keresztül futó információfolyam nagysága világviszonylatban megnégy-

¹ BOTOS ANDOR: *A felhő alapú számítástechnika adatvédelmi kérdései*, Jogi Fórum, 2015.

szereződik – derül ki a most másodszor publikált Cisco Global Cloud Index felmérésből.² A kieleződő gazdasági verseny makroszinten az országoktól, mikroszinten a vállalkozásoktól megköveteli, hogy minél gyorsabban reagáljanak a környezeti változásokra. A technológiai fejlődés ütemével nehéz lépést tartani, azonban a forradalmi újítások felismerése és rövid időn belüli adaptációja fordulópont lehet a szervezet életében. Adott ország és vállalkozás IT-fejlettsége, a felhőalapú technológia használata tulajdonképpen jelzi annak innovációs képességét is, hiszen a megfelelő eszközök hiányában lehetetlen újítani.

A felhőalapú technológia számos területen nyújt támogatást egy ország és egy vállalkozás számára. Egyre jelentősebben járulnak hozzá az állampolgárok életminőségének, a vállalkozások versenyképességének és az állami működés hatékonyságának javulásához.³

Segítségével többek között javítható az adócsalások felderítése a NAV-nál,⁴ optimalizálhatók a termelési folyamatok a vállalkozásoknál.⁵ Megkönnyíthető a kommunikáció, felgyorsul az információáramlás, hatékonyabbá válik az adatfeldolgozás. Egy informatikai részleg üzemeltetése azonban kihívásokat is rejt magában. A számítástechnikai infrastruktúra kiépítése egyrészt tökeigényes feladat, nem beszélve a további karbantartási, fejlesztési költségekről. Másrészt a rendszer fenntartása nagyfokú szaktudást igényel, ami megjelenik vezetői és alkalmazotti szinten is.

2. A FELHŐALAPÚ SZÁMÍTÁSTECHNIKA FOGALMA ÉS TÍPUSAI

A „cloud” azaz a „felhő” kifejezés a grafikus ábrázolásból ered, ez valójában egy szimbólum. Az informatikai ábrákon ezzel a piktogrammal jelölik a külső szolgáltatásokat, amellyel az ábra többi eleme kapcsolatot tart, tehát ezeket a szolgáltatásokat nem egy meghatározott helyről, hanem a „felhőből” lehet elérni.⁶ Az angol „cloud computing”, elnevezésből származó számítástechnikai gyűjtőfogalmat többféleképpen is megközelíthetjük. Repschläger és Zarnekow szerint „a felhőalapú számítástechnika olyan szolgáltatások, alkalmazások és erőforrások sokasága, melyeket a felhasználónak flexibilisen és skálázhatóan (testre szabhatóan) az interneten keresztül ajánlanak anélkül, hogy egy hosszú távú tökelekötés és IT-specifikus know-how lenne szükséges. A felhasználó a vertikális integrációs mélység függvényében vagy egy komplett szoftveralkalmazást, vagy csak a szükséges IT-inf-

2 Cisco Global Cloud Index: *Forecast and Methodology*, 2014–2019, 2015. Forrás: www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf (2015. 10. 01.)

3 NISZ Zrt.: *Az infokommunikációs szektor fejlesztési stratégiája* (2014–2020) v9.0, 2014. Forrás: www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf (2015. 11. 01.)

4 VÁGÚJHELYI Ferenc: *A Big Data és a NAV – Üzleti döntéstámogatás az adatforrástól a vizualizációig konferencia*, 2015. február 18., IIR Magyarország

5 BÖGEL György: *Az informatikai felhők gazdaságtana – üzleti modellek versenye az informatikában*, Közgazdasági Szemle, 56(2009)/673–688.

6 LEPENYE Tamás: *Számítási felhő – egyszerűen* = Lepenye Tamás webnaplója, 2011. június 15. Forrás: lepenyet.wordpress.com/2011/06/15/szmtsi-felho-egyszeruen/ (2015. 10. 01.)

rastrukturát tudja igénybe venni.”⁷ Buyya és munkatársai a következőképpen értelmezik a felhőalapú számítástechnika fogalmát: „A felhő a párhuzamos és osztott rendszereknek egy típusa, amely összekötött és virtuális számítógépek gyűjteményéből áll, amelyek dinamikusan ellátottak és megjelenítettek egy vagy több számítógépes erőforrásként, amely olyan szolgáltatási szinteken alapul, amiket a szolgáltatást biztosító és a fogyasztó közötti tárgyalásokon alakítottak ki.”⁸ A felhőalapú számítástechnika az informatika közművesítésének egy újabb lehetséges eszköze.⁹ Az informatika mint közmű fogalmát John McCarthy vezette be.¹⁰ 1961-ben megjósolta, hogy az informatika egyszer ugyanolyan szolgáltatás lesz, mint bármely más közmű-, a víz- vagy a villanyszolgáltatás.¹¹

A szervezeti igényekhez igazodva eltérő felhőalapú szolgáltatásmodellek jelentek meg. A szakirodalom három alapvető modellt különböztet meg:^{12,13}

- az *Iaas*, vagyis infrastruktúra mint szolgáltatás;
- a *Paas*, platform mint szolgáltatás;
- és a *Saas*, szoftver mint szolgáltatás.

Az *Iaas*, a felhőalapú szolgáltatásmodellek „alapszintje”. A szolgáltató szempontjából ez azt jelenti, hogy valaki a virtualizált környezetben a virtuális gépeket mások számára – díj fejében – átadja. Előfordul, hogy házon belül is alkalmazzák ezt a metódust a jobb erőforrás-kihasználtság és a költséghatékonyság érdekében.

A *Paas*-megoldások olyan fejlesztési platformok, melyeknél a fejlesztési eszközök a felhőben hosztoltak és webböngészőn keresztül elérhetőek, mint a *Saas*-megoldások. A *Paas* segítségével a fejlesztők akár anélkül is tudnak webes alkalmazásokat fejleszteni, hogy bármilyen eszközt is telepítettek volna a gépükre, majd telepíthetik ezeket az alkalmazásokat a *Paas*-kiszolgálókra minden speciális rendszeradminisztrációs háttértudás nélkül.

A *Saas* alatt olyan független szolgáltató által fejlesztett és hosztolt szoftvereket értünk, melyeket a végfelhasználó az interneten keresztül ér el és előre meghatározott licenccdíj fejében vehet igénybe. Szemben a hagyományos szoftverekkel, a *Saas*-megoldásokat a végfelhasználó nem telepíti fel a saját számítógépeire vagy szervereire, azok a szolgáltató tulajdonában maradnak és a saját adatközpontjában, a saját gépein futnak.

7 Jonas REPSCHLÄGER, Rüdiger ZARNEKOW: *Studie: Cloud Computing in der IKT-Branche, Status-quo und Entwicklung des Cloud Sourcing von KMUs in der Informations- und Kommunikationsbranche in der Region Berlin Brandenburg*, Universitätsverlag der TU Berlin, 2011.

8 Rajkumar BUYYA, Chee Shin YEO, Srikumar VENUGOPAL, James BROBERG, Ivona BRANDIC: *Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*, 2009. Forrás: www.researchgate.net/publication/222410212_Cloud_computing_and_emerging_IT_platforms_Vision_hype_and_reality_for_delivering_computing_as_the_5th_utility (2015. 10. 01.)

9 HORVÁTH Katalin, KÖNIG Balázs, ORBÁN Anna, TÖRLEY Gábor: *A közigazgatási informatika alapjai*, Nemzeti Közszerkeleti és Tankönyv Kiadó Zrt., Budapest, 2013, 198.

10 John MCCARTHY: *A basis for a mathematical theory of computation, preliminary report*, apers presented at the May 9–11, 1961, western joint IRE-AIEE-ACM számítástechnikai konferencia, 1961.

11 RACSKÓ Péter: *A számítási felhő az Európai Unió egén*, *Vezetéstudomány*, 43(2012)/1.

12 Chris HARDING: *Cloud Computing for Business – The Open Group Guide*, The Open Group, Van Haren Publishing, 2011.

13 Frank FISCHER, Freda TURNER: *Cloud Computing as a Supply Chain, Business Operations-Systems Perspectives in Global Organizations* (DDBA – 8110 – 7), Walden University, 2009. 10. 07.

Az üzleti szférában az IaaS-re jellemző példa az Amazon Elastic Cloud Computing szolgáltatása, ahol virtuális számítógépeket vehetünk igénybe igen rugalmas konfigurációban. A Microsoft elsősorban a .Net platformon kínál szolgáltatásokat (PaaS), míg a Google a vállalati levelezést, irodai munkát támogató eszközöket, dokumentumtárolást és szerkesztést kínálja szolgáltatásként (SaaS).¹⁴

A közszférában jó példa a SaaS-re az önkormányzati ASP. Az alkalmazásszolgáltató (Application Service Provider – ASP) központon keresztül olyan hardver- és szoftver-infrastruktúra, arra épülő keret- és szolgáltatási rendszer jön létre, mely által az önkormányzatok az alábbi szolgáltatásokat vehetik igénybe: gazdálkodási, ingatlanvagyon-kataszter, önkormányzati adó-, iratkezelő, önkormányzati portál és ipari, kereskedelmi rendszer.¹⁵ A PaaS- és az IaaS-használatra példa lehet az egészségügy. Az eRecept, az eHR, az elektronikus adatcsere ma már alapkövetelmény, az elektronikus beutaló sem új innováció, az informatikai fejlesztések lassan beérő eredményei azonban sokat javítanak az egészségügyi ágazat helyzetén. Bár stratégiai jelentőségű adatvagyonról van szó, már csak az adatvédelmi kérdéseket kell annak érdekében tisztázni, hogy az adatok a rendszer működését és a forrásteremtést egyaránt szolgálhassák.¹⁶

A National Institute of Standards and Technology (NIST) alapján a számítási felhők kialakításának négy alaptípusát különböztethetjük meg, melyek a következők: magán-, közösségi, nyilvános és hibrid felhő.¹⁷ Ezek jellemzői:

- A *magán-* (vagy *privát-*) *felhő* egyetlen szervezet részére fenntartott felhő-infrastruktúra üzemeltetését jelenti. A magánfelhőt birtokolhatja és működtetheti adott szervezet, a szolgáltató, egy harmadik fél vagy azok bármilyen egyéb kombinációja. Kialakíthatják a vállalat telephelyén, valamint azon kívül is.
- A *közösségi felhő*t egy adott közösség, vállalkozások vagy szervezetek egy csoportja használja, akiket valamilyen közös érdek köt össze.
- A *nyilvános felhő* a nagyközönség számára nyitott, bárki felhasználhatja. Birtokolhatja és üzemeltetheti üzleti szervezet, akadémiai vagy kormányzati szervezet, vagy ezek kombinációi. A felhőszolgáltató telephelyén belül van kialakítva.
- Végül a *hibrid felhő* két vagy több különböző cloud-infrastruktúra (magán-, közösségi vagy nyilvános) szabványosított, védett technológián alapuló összekapcsolása. Az összekapcsolás valamilyen cél érdekében történik, pl. hatékonyságnövelés, üzemeltetési terhelés ki egyenlítése, adatok, alkalmazások hordozhatósága.

14 RACSKÓ: *i. m.*, 2012.

15 Sajtóközlemény: Önkormányzati ASP központ felállítása, Kormányzati Informatikai Fejlesztési Ügynökség, 2013

16 TARCZA Orsolya: *Hangsúlyeltolódások a központi e-Health fejlesztésekben*, Medicalonline.hu, 2015. Forrás: www.medicalonline.hu/eu_gazdasag/cikk/hangsulyeltolodasok_a_kozponti_e_health_fejlesztésekben (2015. 10. 01.)

17 Peter MELL, Timothy GRANCE: *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, NIST honlap, 2011. Forrás: csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (2015. 10. 01.)

3. A FELHŐALAPÚ SZÁMÍTÁSTECHNIKA HASZNÁLATÁBÓL SZÁRMAZÓ ELŐNYÖK

A felhőalapú számítástechnikát 2005-ben indították el azok a nagy, multinacionális cégek, amelyek hatalmas számítástechnikai erőforrásokkal rendelkeztek saját rendszereik működtetéséhez, például az Amazon, a Microsoft és a Google. Az Európai Unió Statisztikai Hivatala 2014 végén nyilvánosságra hozta a legfrissebb adatokat azzal kapcsolatban, hogy a helyi vállalkozások hány százaléka használ felhőszolgáltatásokat. A felmérésben az Európai Unió 28 tagállama vett részt. Az adatok szerint a tagállamokban átlagosan minden ötödik társaság alkalmaz adatok tárolására vagy más tevékenységekre felhőszolgáltatást, és több mint 80%-uk inkább a saját infrastruktúrájára támaszkodik. 2014-ben majdnem kétszer annyi cég használt nyilvános felhőalapú szervert (12%), mint magánfelhőt (7%) az Európai Unióban.

A legtöbb vállalkozás – a vállalkozások több mint fele – Finnországban él a felhőalapú szolgáltatások nyújtotta lehetőséggel, majd Olaszország, Svédország és Dánia következik. Magyarországon a 23. helyen található, 8%-os használati gyakorisággal.

Az Európai Unió vállalkozásainak kétharmada e-mailezésre, több mint fele fájl tárolásra, harmada irodai szoftverek és pénzügyi alkalmazások működtetésére használja a felhőalapú számítástechnikát.¹⁸

A felhőalapú számítástechnika egyes típusainak megvannak a speciális előnyei, amelyek nagyban függenek a felhasználási céltól. Néhány közülük azonban általánosan érvényes a felhő valamennyi fajtájára. Az alább felsoroltak a legfontosabbak:

– **Költségcsökkentés.** A köz- és az üzemi szférában a költségek tervezésekor külön figyelembe kell venni a beruházások nagyságát, valamint a munkák során felhasználandó SSC (Single Service Company) és egyéb külső vállalkozók által biztosított szolgáltatások költségvonzatait. Ez tovább bontható:

- **Nagyobb tőkeberuházásra** – Capex (capital expenditure) modell – épülő felhőszolgáltatásokra, ami a saját tulajdonú magánfelhő megvalósításánál figyelhető meg.¹⁹ Ez egy egyszeri költség, ami nem írható le azonnal és kockázatos, de alacsony(abb) működési költséggel bír.
- **Informatikai szolgáltatások kiszervezése,** ahol a működtetési költségek – Opex (operational expenditure) modell – rendszeresek, adózás előtt leírhatók, és kevésbé kockázatosak, de az adatátviteli kapcsolat adottságai befolyásoló tényezők.
- **Adatbiztonság, adatvédelem.** A felhőalapú számítástechnika biztonságosabb, mint amit néhány kis- és középvállalkozás (vagy önkormányzat) fel tud mutatni, akik valahol a saját épületeikben tárolják az adataikat. Ráadásul rendkívül drága fenntartani egy biztonsági rendszert. Részben a tisztázatlanságok miatt, részben pedig azért, mert egy új technoló-

18 GIANNAKOURIS Konstantinos, SMIHILY Maria: *Eurostat: Cloud computing – statistics on the use by enterprises*, 2014. november. Forrás: ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

19 GAZDAG Ferenc: *Infokommunikációs rendszerek a közigazgatásban*, Trendek a modern informatikában, előadás a Nemzeti Közszolgálati Egyetemen, 2015. 09. 22.

giai megközelítésről van szó, sok iparágban jogszabály határozza meg, hogy az informatikai infrastruktúra mely elemei kerülhetnek egyáltalán felhőszolgáltatóhoz, és melyek nem (ez az érzékeny adatokat kezelő szervezetek, illetve a valamilyen szempontból kritikusnak minősített infrastruktúrához tartozó közművállalatok esetében jellemző).

- **Hatékonyág.** A felhőalapú infrastruktúrából nyújtott számítási és tárolási kapacitás optimális esetben akár néhány perc alatt az ügyfél rendelkezésére állhat. A kiépített rendszer sajátossága, hogy az időközben felszabaduló kapacitások, szükségtelemné váló erőforrások akár azonnal kiejánlhatóvá, felhasználhatóvá válnak. Igény esetén a szerverek átméretezhetőek, a fizikai erőforrásokból csupán annyit használnak fel, amennyire az adott pillanatban éppen szükség van. Ezzel a megoldással az esetlegesen hirtelen jelentkező többletigények is problémamentesen kezelhetők.

Összetett, komplexebb előnyök:

- **Munkavégzés, szervezeti kultúra változása.** Az új technológia nagyban megváltoztatja a folyamatokat. A szervezeten belül az embereknek el kell fogadniuk, hogy a felhő úgy rendezi át az erőforrásokat, hogy azok támogassák a költségsökkentést, illetve az üzleti növekedést. A felhőalapú számítástechnikához értő tehetségeket meg kell találni: a szervezetnek hosszú távon olyan munkaerőre lesz szüksége, aki képes kiaknázni a felhőben rejlő minden lehetőséget.
- **Versenyképesség javítása.** A felhőalapú szolgáltatások ma már komolyan hatnak a kis- és középvállalkozások működésére. Ezek az „első fecskék” a felhőalapú technológia használatával indítják be vállalkozásaikat vagy projektjeiket, illetve keresik az üzleti siker új lehetőségeit, csökkentik a költségeiket és növelik a hatékonyságot. A technológia egyben új lehetőségeket is kínál: új piacokat tesz elérhetővé, segíti az új üzleti modellek megvalósítását, és az ügyfelek számára is pozitív változásokat hoz. Az üzleti élet mellett a közigazgatás szereplői is felismerik az új technológia előnyeit. Európa kormányai azon dolgoznak, hogy kidolgozzák, a felhőalapú megoldásokkal hogyan növelhető a hatékonyság, miként nyújthatók jobb szolgáltatások, illetve hogyan fokozható a növekedés. Látható, hogy a felhőalapú számítástechnikának köszönhetően Európa egyes országainak polgárai mára hatékonyabb és gyorsabb közigazgatási szolgáltatásokban részesülnek.

Egy osztrák és egy magyar vállalkozásokra kiterjedő kutatás alapján megállapítható, hogy például az osztrák mikro-, kis- és középvállalkozások méretkategóriától függetlenül ugyanazokat az előnyöket ugyanabban a sorrendben érzékelik a felhőalapú technológiában. A legfontosabb számukra a *magas szintű mobilitás* és az *információs rendszerhez való távoli hozzáférés*. A magyar vállalkozásoknál más és más sorrend figyelhető meg. A mikrovállalkozásoknál a *gyorsabb információáramlás*, a kisvállalkozásoknál rendszerösszeomlás esetén a *könnyebb helyreállíthatóság*, a középvállalkozásoknál a *távoli hozzáférés* és a nagyvállalatoknál a *gyorsabb információáramlás* a legfontosabb előny a felhőalapú szolgáltatásnál.²⁰

20 SASVÁRI Péter: *A felhőalapú számítástechnika ismeretének és használatának vizsgálata az ausztriai és a magyarországi vállalkozásoknál II.*, Gazdálkodás és Menedzsment Tudományos Konferencia, Kecskemét, 2015. 08. 27–28. (megjelenés alatt)

A felhőalapú számítástechnika használatának vannak *hátráltató* tényezői. 2014-ben az Eurostat felmérést végzett az Európai Unió országainak körében, a technikai feltételek tekintetében. Első helyen a *lassú hozzáférést vagy használatot*, a második helyen az *eszközök összeférhetetlenségét*, a harmadik helyen a *szerverek fizikai elérhetetlenségét* jelölték meg.

Magyar vállalkozások körében végzett kutatás alapján a nagyvállalatok a *szolgáltatókkal szembeni bizalmatlanságban*, a középvállalkozások a *meglévő alkalmazások áttelepítésének nehézségében*, a kisvállalkozások a *felső vezetés ismereteinek hiányában*, a mikrovállalkozások esetén az *adatvesztés lehetőségében* látják az esetleges problémát.²¹

A közigazgatási alkalmazások esetében – a felhőalapú alkalmazások tekintetében is – az érvényes jogi, szabályozási keretek nem mérlegelhetők.²²

De az leszögezhető, hogy a felhőalapú technológia egy modern innovációs megoldásnak tekinthető. Everett M. Rogers könyvében az innovációk elfogadásának, elterjedésének öt befolyásoló tényezője van:²³

- *relatív előny*: milyen előnyöket nyújt az új megoldás a korábbiakkal szemben;
- *kompatibilitás*: mennyire illeszkedik az innováció a meglévő értékekhez, a korábban megszerzett tapasztalatokhoz, az alkalmazók igényeihez;
- *komplexitás*: mennyire nehéz megtanulni és használni az új terméket;
- *kipróbálhatóság*: könnyen és különösebb kockázatok nélkül kipróbálható-e az újdonság;
- *megfigyelhetőség*: az alkalmazás, illetve annak következményei láthatók-e mások számára?

Könnyen belátható, hogy a felhőalapú számítástechnika terjedése pozitívan hat mind egyik felsorolt tényezőre, megkönnyítve, sőt szükségessé téve az internetes szolgáltatások innovációjának szervezeti elterjedését. A felhőből nyújtott közigazgatási szolgáltatások megjelenésével az emberek azokkal a megoldásokkal találkoznak, amelyeket már megszoktak és megtanultak.²⁴

4. KONKLÚZIÓ

A digitális eszközök és szolgáltatások terén az uniós polgárokra és vállalkozásokra még számos kiaknázatlan lehetőség vár. Az online vásárlástól és tanulástól kezdve a számlabefizetésen át egészen az online hivatali ügyintézésig a világháló a legjobb megoldás, ha ehhez adottak a feltételek.²⁵

21 SASVÁRI Péter, NAGYMÁTÉ Zoltán: *The Empirical Analysis of Cloud Computing Services among the Hungarian Enterprises = Handbook of Research on Cultural and Economic Impacts of the Information Society*, szerk. Thomas P. E., M. Srihari, Sandeep Kaur, IGI Global, Hershey, 2015, 121–150.

22 RACSKÓ Péter: *A felhőalapú számítástechnika az elektronikus közigazgatásban = E-közzszolgáltatásfejlesztés: Elméleti alapok és tudományos kutatási módszerek*, szerk. Nemeslaki András, Nemzeti Közzszolgálati Egyetem, 2014, 191–209.

23 Everett M. ROGERS: *Diffusion of Innovations*, Free Press, New York, 2003.

24 BÖGEL: *i. m.*, 2009

25 Európai Bizottság – sajtóközlemény: *Mennyire digitális országban él Ön? – A legfrissebb adatok szerint Európának van még mit fejlődnie*, Európai Bizottság, IP/15/4475, 2015. Forrás: europa.eu/rapid/press-release_IP-15-4475_hu.htm

A felhőalapú számítástechnika egy rugalmas és adaptálható IT-környezet létrehozásával segíti a köz- és üzleti szektort folyamataik és technológiájuk átalakításában, hogy így gyorsan megfelelhessenek a változó követelményeknek.

Elmondható, hogy a felhőalapú informatikai rendszerek megjelenése és használata megkerülhetetlen mind a két szektor esetében. A nagy kormányzati beruházások nyomán kialakult, kialakuló sokfajta és széles szolgáltatási palettát kínáló felhőalapú informatika az eddigieknél olcsóbban képes a jelenlegi számítástechnikai igények kielégítésére, vagy akár a meglévőkénél több, újabb feladat ellátására.²⁶

A technológia használatának legfontosabb előnyei a költséghatékonyság, az adatvédelem, a távoli hozzáférés, és a gyors üzembe helyezés. Bevezetésének akadályaként általában a megbízhatóságot, a szolgáltató felé való elköteleződést, az irányítás elvesztését, továbbá a rendszer elérhetőségében beálló esetleges zavart említi a szakirodalom.

A közigazgatási alkalmazások előnyei és hátráltató tényezői abban különböznek az üzleti szférától a felhőalapú alkalmazások tekintetében, hogy míg az üzleti alkalmazásoknál az előnyök és a hátrányok mérlegelésére van mód, addig a közigazgatásban az érvényes jogi, szabályozási keretek nem mérlegelhetők.



SUMMARY IN ENGLISH: The essence of using cloud computing is that the user is not required to possess and maintain sophisticated IT infrastructure within the organization. Such internet based services have a number of benefits. Among others, cost reduction, data protection, improvement in efficiency, cultural change in the organization and an increase in competitiveness both for the public and private sectors. The setbacks of the spread of cloud computing can be of technical and human nature. In the EU it varies from country to country how widespread the use of cloud computing is in the private sector. Today there are a number of new IT services available in the Hungarian public sector.

²⁶ Kovács Zoltán: *Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél*, Hadmérnök, 6(2011. dec.)/4.

Prof. Dr. Nemeslaki András (Nemeslaki.Andras@uni-nke.hu): az NKE E-közzszolgálat Fejlesztési Intézetének vezető egyetemi tanára, okleveles gépészmérnök, a műszaki tudomány kandidátusa. Harminc éve az információrendszer-menedzsment és projektmenedzsment területen végez kutató- és oktatómunkát. Az NKE Közigazgatás-tudományi Doktori Iskolájának törzstagja, de aktívan közreműködik a Budapesti Corvinus Egyetem Gazdaságinformatikai Doktori Iskolájában is oktatóként és témavezetőként is. Tagja a Belügyminiszter E-közigazgatási Tanácsadó Testületének és a NISPAcee E-government Working Group társelnöke. Számos külföldi egyetemen oktatott, ezek közül kiemelkednek a Bocconi University, a Kölni Egyetem, a University College Dublin, valamint a Case Western Reserve Egyetem Clevelandben és a University of Delaware.

Dr. Sasvári Péter (petersasvariphd@gmail.com): egyetemi docens, elsőként gépészmérnöki, majd okleveles közgazdász diplomát, azt követően a társadalomtudományok, gazdálkodás- és szervezéstudományok területén PhD-fokozatot szerzett. A doktori dolgozatának címe „Az információs és kommunikációs technológia fejlettségének empirikus vizsgálata” volt, amit „summa cum laude” minősítéssel 2009-ben védett meg. Fő kutatási területe a közszféra és a vállalkozások információsrendszer-használatának vizsgálata. Primer kutatást végzett külföldi egyetemek bevonásával a kis- és középvállalkozások körében Ausztriában, Bosznia-Hercegovinában, Csehországban, Horvátországban, Lengyelországban, Magyarországon, Németországban, Olaszországban, Spanyolországban és Szlovákiában. Az elmúlt évek tudományos munkásságáról elmondható, hogy több mint 75 közleményből 19 nemzetközi folyóiratban jelent meg, idézettségének száma meghaladja az ötvenet, 5 nemzetközi könyv szerzője volt. 2013. október 1. óta dolgozik a Nemzeti Közzszolgálati Egyetemen. Sasvári Péter az NKE oktatási tevékenységébe is bekapcsolódott. A „Tudománymetria és publikációs stratégia – fókuszban az infokommunikációs technológiák” doktori tárgy oktatásában és a tananyag fejlesztésében aktívan is részt vett.

szakmai fórum •

Nagyné Takács Veronika – Kovács László

AZ INFORMÁCIÓBIZTONSÁGI VEZETŐ SZAKIRÁNYÚ TOVÁBBKÉPZÉS TAPASZTALATAI

Az információ biztonsága napjaink egyik legfontosabb tényezője. Ennek megteremtése a közigazgatásban is kiemelt feladat. Ugyanakkor az információbiztonság megvalósítása és folyamatos fenntartása nem csak technikai kérdés. Ennek megfelelően az információért felelős közigazgatási vezetőktől kezdődően az információt kezelőkig a folyamatos oktatás és felkészítés ezen a területen is elengedhetetlen. A Nemzeti Közszerződési Egyetemen 2014-ben indultak azok a képzések, amelyeket az információbiztonsági törvény a hatálya alá tartozó szervezetek esetében az elektronikus információs rendszer biztonságáért felelős személyek számára kötelezően előír. A képzéssel kapcsolatos tapasztalatok összegzését kiegészítheti az egyik végzett évfolyam nyilvános szakdolgozatainak értékelése, visszajelzést adva a képzést szervező és a jogalkotó számára is. Jelen dolgozat a 2015-ben készült és hozzáférhető, nyílt szakdolgozatok elemzésére épít.

KULCSSZAVAK:

információbiztonság, oktatás, képzés, Nemzeti Közszerződési Egyetem – information security, education, training, National University of Public Service



1. BEVEZETÉS

Ma az élet minden területén számítógépek segítségével gyűjtjük, dolgozzuk fel és használjuk a mind nélkülözhetetlenebbé vált információinkat. Társadalmunk minden szegmensét áthatja az az igény, hogy az információ biztonsága azt az elvárt mértéket képviselje, amely alapján valóban kiegyensúlyozottan működik minden társadalmi funkciónk és ezek minden egyes folyamata.

Az információbiztonságra ma már mint valódi tudományra tekinthetünk, amelynek alapja kétségtelenül maga az információtudomány. Ugyanakkor az információtudományban meglévő elveket ki kell egészítenünk a biztonság különböző tudományos igénnyel feltárt

kérdéseivel. Mivel napjainkban az információs rendszerek megfeleltethetőek számítógép-hálózatoknak és számítógéprendszereknek, ezért nagyon sokszor egyszerű technikai, ebben az esetben informatikai kérdésnek tekintjük az információbiztonságot.

Ez azonban csak részben igaz, hiszen az információ kezelésében jelen van az ember is, ami azonnal magával hozza a kérdés humán összetevőinek a vizsgálatát is. Ennek megfelelően ma az információbiztonságot alapvetően komplex megközelítésben kell alkalmazni, azaz figyelmet kell fordítani a fizikai, a humán, az adminisztratív és az elektronikus biztonsági összetevőkre egyaránt.

Mindezek a közigazgatásra hatványozottan igazak. A közigazgatásban megjelenő információk esetében az ágazat funkcióiból eredően megkérdőjelezhetetlen módon jelentkezik az információk bizalmassága és sértetlensége, valamint azok rendelkezésre állása.¹ Van azonban egy komoly probléma az információbiztonság közigazgatásban történő mérésével, mivel itt az esetek igen nagy százalékában a biztonság hiánya miatt esetlegesen bekövetkező károk nem, vagy csak nagyon nehezen – akkor is csak közvetett módon – fejezhető ki anyagi veszteségként. Természetesen, ha például az állampolgárok bizalomvesztését mint kárt tekintjük, máris bizonyos mértékben mérhetővé válik a biztonság minősége.

Minden fejlett ország természetesen ma már szabályozza az információbiztonság megteremtését és fejlesztését a stratégiai szinttől egészen a konkrét technikai vagy akár a humán összetevők szabályozásáig. Ezek az információbiztonsági szabályozók kiemelten kezelik a felkészítés és az oktatás kérdését. Így van ez hazánkban is.

Ennek megfelelően épül fel jelen írás is, amely a hazai információbiztonsági képzések közül egyet, nevezetesen az információbiztonsági vezető szakirányú továbbképzést emeli ki és vizsgálja meg, korántsem a teljesség igényével.

Jelen tanulmány mottójául a következők szolgáltak: *A tanulás célja – túl a tanulás nyújtotta gyönyörűsége – az, hogy a jövőben hasznunk legyen belőle* (Jerome Seymour Bruner amerikai pszichológus).

2. AZ INFORMÁCIÓBIZTONSÁG JELENTŐSÉGE ÉS SZABÁLYOZÁSA

Mindennapi életünket átszövi a számítógépes rendszerek. Ma nagyon nehéz elképzelni bármilyen társadalmi funkciót számítógépekre alapozott információs folyamat nélkül. Ahogy korábban utaltunk rá, ez a közigazgatás esetében sincs másképp. Természetesen az egyes szereplők nem egyformán érintettek a folyamatokban, ennek megfelelően az informatikai rendszerek biztonsága sem érint mindenkit egyforma mértékben. Az azonban ma elvitathatatlan tény, hogy az egyszerű felhasználó, vagy az egyszerű ügykezelő is fontos szereplője és aktív részese a biztonságnak. Ennek oka elsősorban az, hogy az információtechnikai és -technológiai biztonsági kérdéseket leszámítva (és még azok közül sem mindegyiket lehet a felhasználók felelősségi köréből kivonni) a felhasználó felkészültsége, képzettsége és ezzel (akár) egye-

1 Az információbiztonság szakmai terminológiájában az angolul confidentiality, integrity, availability, azaz bizalmasság, sértetlenség, rendelkezésre állás a legfontosabb alapelvek közé tartoznak. Az angol szavak kezdőbetűiből alkotott CIA elvként is ismert ez a fogalomhármas.

nes arányban álló biztonságtudatossága kulcskérdés, mert az ember az, aki a legtöbbet tudja tenni az információk biztonságának megteremtéséért.

Az információbiztonság korábban jelzett komplex megvalósítása, azaz a fizikai, adminisztratív, humán és elektronikus információbiztonság szükségessé teszi mind nemzetközi, mind nemzeti szabályozás kialakítását. Mindezen területek a nemzetközi szervezetek – pl. NATO vagy az Európai Unió –, de akár egy adott ország esetében is a kibertér biztonságának megteremtésével kezdődik, mivel az információbiztonság egyik legfontosabb dimenziója a kibertér.

A NATO a 2007-es észti incidens² óta kiemelt kérdésként kezeli a kibertérben zajló tevékenységeket. A NATO 2010-es lisszaboni csúcstalálkozója után a szövetség stratégiai koncepciójában szerepelteti, hogy az egyre szofisztikáltabb számítógépes támadások miatt a szövetség információs és kommunikációs rendszereinek védelme az egyik legsürgősebb feladat.³

Az Európai Unióban 2013 év elején jelent meg az Unió új kiberbiztonsági stratégiája, amelyet az EU külügyi és biztonságpolitikai főképviselője és az Európai Bizottság közösen dolgozott ki. Az Európai Unióban ez az első olyan átfogó stratégia kibertérre, amelyet az EU a kiberbiztonság területén megalkotott.⁴ A stratégia nagyon egyértelmű célokat és prioritásokat tűz ki az EU nemzetközi kibertér-politikája terén, amelyek között a szabadság és nyitottság, a jogkövetés, a kiberbiztonsági kapacitások kiépítése, valamint a kibertérrel kapcsolatos nemzetközi együttműködés ösztönzése is megjelenik.⁵ Ezt követően 2014 novemberében született meg az EU kibervédelmi politikai keretrendszere, amely már több mint 40 jól megfogalmazott akciót fogalmaz meg a kibervédelem megvalósítása és növelése érdekében.⁶ Ezek közül az egyik legfontosabbnak tekinthető a kibervédelmi képzések, oktatások és gyakorlatok megvalósítását szorgalmazza.

Magyarországon a biztonsági stratégiai dokumentumokban először 2012-ben jelent meg markáns módon a kibertér, mint olyan tényező, amelyre különös figyelmet kell fordítani. A 2012-ben megjelent új Nemzeti Biztonsági Stratégiában kiemelt helyen található a kiberekívások jelentette veszélyeket.⁷ Ez a stratégia rendkívül előremutató, hiszen álmamilag elfogadott, a nemzet biztonságát meghatározó stratégiai elvek először tartalmazzák e terület fontosságát és védelmének szükségességét.⁸ A stratégia természetesen felméri a terület veszélyforrásait: „Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem

2 2007 tavaszán feltehetően orosz elkövetők komoly kibertámadásokat intéztek a fejlett észti internetes infrastruktúra ellen.

3 A NATO 2010-es új stratégiai koncepciója: Aktív Szerepvállalás, Modern Védelem. Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról.

4 Kovács László: *Biztonságpolitika = E-köszolgáltatásfejlesztés: Elméleti alapok és tudományos kutatási módszerek*, szerk. NEMESLAKI András, Nemzeti Köszolgálati Egyetem, Budapest, 2014, 227–248, 245. (ISBN 978-615-5491-04-7)

5 EC Cybersecurity Strategy, 2013.

6 EU Cyber Defence Policy Framework, 2014.

7 Nemzeti Biztonsági Stratégia, 2012.

8 Kovács: *i. m.*, 241.

állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését.”⁹

2013 elején a Kormány elfogadta a nemzeti kiberbiztonsági stratégiát.¹⁰ A stratégia összhangban az EU-s ágazati stratégiával, az oktatás és képzés kérdésén szintén kiemelt helyen kezeli, hiszen előírja annak szükségességét, hogy „a kiberbiztonsági oktatás, képzés, valamint a kutatás és fejlesztés színvonala megfeleljen a legjobb nemzetközi gyakorlatoknak, hozzájárulva egy világszínvonalú hazai tudásbázis kialakításához.”¹¹

A nemzeti kiberbiztonsági stratégia alapelveire épülve született meg *Az állami és önkormányzati szervek elektronikus információbiztonságáról* szóló 2013. évi L. törvény, azaz a szakma által csak információbiztonsági törvénynek (Ibtv.) nevezett jogszabály. Ez a törvény alapvető változásokat hozott a hazai információbiztonság szervezeti kereteiben, valamint nagyon egyértelmű szabályozást ad a hazai információbiztonsági képzés és oktatás területére.

3. HAZAI INFORMÁCIÓBIZTONSÁGI KÉPZÉS

Az Ibtv. a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon és az ezt kezelő információs rendszerek védelme érdekében kiemelt figyelmet fordít arra, hogy a törvény hatálya alá tartozó szervezetek információbiztonsággal foglalkozó munkatársai megfelelő ismeretek birtokában lássák el feladataikat.¹²

Az Ibtv. és a 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról (képzési rendelet) az érintett munkatársak számára egyrészt a munkakör betöltéséhez szükséges végzettségre, illetve szakmai tapasztalatra vonatkozó előírásokat rögzít, másrészt a Nemzeti Közzolgálati Egyetem (NKE) által szervezett képzéseken, továbbképzéseken történő részvétel kötelezettségét írja elő.¹³

A Nemzeti Közzolgálati Egyetem Vezető- és Továbbképzési Intézete (VTKI) keretei között megvalósuló *Elektronikus információbiztonsági vezető szakirányú továbbképzési szak* második végzett évfolyamának eredményeit a szak minőségbiztosítási rendszerének megfelelően értékeli a szak vezetői és oktatói, valamint az egyetem érintett munkatársai, továbbá a hallgatók is.

Ugyanakkor jelen előzetes értékelés során, amely alapvetően a hallgatók szakdolgozatainak elemzésére épül, több olyan következtetés is levonható, amelyek mind a további képzések szervezése, mind az információbiztonsággal összefüggő jogalkotás során hasznosíthatóak lehetnek.

9 Nemzeti Biztonsági Stratégia, 2012.

10 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

11 *Uo.*

12 KRASZNY Csaba, SZÁDECZKY Tamás: *Az információbiztonság és állami szabályozása = E-közzolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek*, szerk. NEMESLAKI András Nemzeti Közzolgálati Egyetem, Budapest, 2014, 353, 249–264. (ISBN 978-615-5491-04-7)

13 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

4. AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI VEZETŐ SZAKIRÁNYÚ TOVÁBBKÉPZÉS TARTALMA

Az *Elektronikus információbiztonsági vezető szakirányú továbbképzés* az elektronikus információs rendszerek védelméért felelős vezető, az elektronikus információs rendszerek biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek szakirányú továbbképzése.¹⁴ A képzés¹⁵ fő célja – a Nemzeti Közzolgálati Egyetem honlapján közzétett információ szerint – „az Ibtv.-ben meghatározott elektronikus információs rendszer biztonságáért felelős személyek feladatellátáshoz szükséges szakmai kompetenciáinak átadása és a biztonságtudatos szemléletmód kialakítása”¹⁶

A képzés kialakítása során az Information Systems and Control Association (ISACA) nemzetközi szervezet Certified Information Security Manager (CISM) képzését vették alapul. Mindazonáltal „a nemzetközi trendek is alátámasztják, hogy az információbiztonság nemcsak technológiai, hanem elsősorban szervezati irányítási kérdés, erős jogi-közigazgatási fókusszal”, ezért „a képzés – bár az információbiztonság műszaki, informatikai szakterületnek tűnik – egy speciális, információbiztonságra koncentrálnak menedzserképzés”¹⁷

A fenti állítást a magyar és nemzetközi közigazgatási,¹⁸ valamint kutatási tapasztalatok¹⁹ is alátámasztják. Az Ibtv. szerint a felelős vezető mellett (aki lehet a szervezet első számú vezetője vagy az általa kijelölt, megbízott „egyéb” vezető) kiemelt felelőssége van az információbiztonságért felelős személynek is. Az Ibtv. hatálya alá tartozó szervezetek esetében az ő feladatait jellemzően vagy a jogi-igazgatási szakterület vezetőjére/munkatársára telepítik (az adatvédelem hagyományosnak tekinthető feladatcsoportját bővítve ezzel), vagy az informatikai szakterület vezetőjére/munkatársára (mivel informatikai szakmai ismeretekkel végzettségéből fakadóan ő rendelkezik). A képzés tartalma összeállításának nehézsége ebből a kettősségből fakad. Az informatikai szakmai részt úgy kell összeállítani, hogy egy szakmabelinek is adhasson hasznosítható ismeretet, de az informatikától, mint konkrét szakmai feladatoktól kissé távolabb álló szakterület munkatársai számára is befogadható legyen, ugyanakkor a jogi-igazgatási szakmai rész címzettjei lehetnek jogászok, igazgatási szakon végzetek többéves jogi képzéssel

14 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról (Képzési rendelet)

15 A képzési rendelet ezt az oktatási formát nevezi *képzésnek*; ezen kívül rendelkezik az egyszer teljesítendő *továbbképzésről* és az éves *továbbképzésről*.

16 vtki.uni-nke.hu/szakiranyu-tovabbkepzes/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto-szakiranyu-tovabbkepzesi-szak (2015. 10. 12.)

17 ILLÉSY Miklós, NEMESLAKI András, SOM Zoltán: *Elektronikus információbiztonság-tudatosság a magyar közigazgatásban*, Információs Társadalom, 14(2014)/1, 52–73.

Forrás: www.infonia.hu/digitalis_folyoirat/2014/2014_1/i_tarsadalom_2014_1_illessy_nemeslaci_som.pdf

18 NEMESLAKI András: *Vállalati internetstratégia*, Budapest, Akadémiai Kiadó, 2012, 271. (ISBN 978-963-05-9189-8)

19 SASVÁRI Péter, NEMESLAKI András, WOLF RAUCH: *Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises*, Academic and Applied Research in Public Management Science, 14(2015)/1, 63–78.

a hátuk mögött és olyan informatikusok is, akiknek jogi-igazgatási ismeretei szinte egyáltalán nincsenek, így számukra ezen a területen a legelemibb ismeretek átadása is szükséges.

A képzési idő a jogszabály alapján két félév (300 óra, ennek 80%-a elmélet, 20%-a gyakorlat), a képzés szakdolgozat megírásával és megvédésével, valamint záróvizsgával zárul. Ebben a képzésben alapképzésben vagy mesterképzésben szerzett oklevéllel rendelkezők vehetnek részt, amennyiben rendelkeznek angol nyelvű alapfokú komplex nyelvvizsgával vagy ezzel egyenértékű bizonyítvánnyal. Ez utóbbi feltétel indoka, hogy az információbiztonsági szakirodalom jelentős hányada angol nyelven érhető el, tanulmányozása ugyanakkor szükséges a naprakész ismeretek megszerzéséhez, következménye viszont, hogy az esetleg több nyelvből nyelvvizsgával rendelkező, esetenként még angol nyelvismerettel is bíró, de azt oklevéllel, bizonyítvánnyal igazolni nem tudó foglalkoztatottak, munkavállalók kiesnek a fellevehető személyek köréből. Mindezek igazak úgy, hogy munkakörük betöltéséhez az angol nyelv említett dokumentumokkal igazolt ismerete nem is feltétlenül szükséges.

A képzés tárgykörei:²⁰

- információbiztonsági szervezési ismeretek;
- kockázatértékelés és -menedzsment;
- stratégia és szervezeti támogatás;
- biztonsági események kezelése (incidenskezelés);
- jogi, vezetéselméleti és technológiai ismeretek az információbiztonságban.²¹

A képzés tananyaga 2014-ben, az *ÁROP-2.2.21 Tudásalapú közszolgálati előmenetel* projekt keretein belül készült és az alábbi témaköröket foglalja magában:

- A minőségirányítás alapjai;
- Biztonsági technológiák alkalmazása;
- Biztonsági tesztelés a gyakorlatban;
- Biztonságpolitika;
- Biztonság támogatása;
- Biztonságtechnika;
- Hálózatok biztonsága;
- Incidensmenedzsment, BCP, DRP integráció;
- Incidensmenedzsment gyakorlat;
- Információbiztonsági program;
- Információbiztonsági stratégia és vezetés;
- Információbiztonsági szabványok;
- Információbiztonság-tudatosság gyakorlat;
- Irányítási rendszerek;

20 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról (Képzési rendelet)

21 Az egyetem honlapja szerint a megszerzhető tudáslemek: Alapismeretek – jogi, vezetéselméleti és technológiai ismeretek, Stratégia és szervezettámogatás – Rendszerirányítási szakismeretek, Információbiztonsági szervezési szakismeretek, Információkockázatok kezelése és a megfelelés, Információbiztonsági események kezelése (incidenskezelés) ismeretek. (2015. 10. 12.)

- Jogi és közigazgatási ismeretek;
- Kockázatértékelés, kockázatmenedzsment;
- Kockázatmenedzsment gyakorlat.

A képzés tartalmának optimalizálásához figyelembe kell venni azt is, hogy a célközönség számára a képzési rendelet további rendszeres továbbképzést is előír. Évente továbbképzésen kell részt vennie 8 óraban a vezetőnek, 25 óraban az információbiztonság megvalósításában közreműködőnek és 50 óraban az információbiztonságért felelős személynek. Ez utóbbi továbbképzés tárgykörei:

- információbiztonsági technológiai ismeretek;
- kockázatértékelés és biztonsági események kezelése (incidenskezelés);
- informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek;
- jogi és szervezeti irányítási ismeretek.²²

Első ízben ezt a továbbképzést szintén a Nemzeti Közszolgálati Egyetem szervezte meg 2014-ben, amely képzés e-learning keretében történt és vizsgával zárult. A továbbképzés elvégzéséről a résztvevők tanúsítványt kaptak. A tananyag az alábbi részekből állt:

- Kriptográfia;
- Alkalmazásbiztonság;
- Sebezhetőségvizsgálatok a gyakorlatban;
- A személyes adatok védelmének szabályozási környezete és gyakorlati kérdései;
- Elektronikus dokumentumok kezelése, hitelesítése, megőrzése.

A 2015-ben sorra kerülő továbbképzésben – a hallgatóknak e-mailben megküldött tájékoztató szerint – a tananyag (értelemszerűen), az oktatás módja és a számonkérés is módosult. A tananyag jogi-közigazgatási ismereteket tartalmazó részét személyes jelenléti (tantermi) oktatás keretében kell elsajátítani (mivel a 2015 nyarán bekövetkezett jelentős jogszabályváltozásokról még nem áll rendelkezésre hatályos tananyag), a számonkérés formája házi dolgozat. A tananyag:

- Jogi és közigazgatási ismeretek;
- Kockázatmenedzsment;
- Biztonsági technológiák alkalmazása.

5. A KÉPZÉSEN VÉGZETT MÁSODIK ÉVFOLYAM MEGISMERHETŐ SZAKDOLGOZATAI

Az első évfolyamon 2014. február és 2015. január között 30 fő képzése történt meg, 29 hallgató zárta sikeresen a tanulmányait. A jelen tanulmányban szereplő szakdolgozatokat készítő hallgatók képzése a 2014–2015-ös tanulmányi évben zajlott, 25 fő részvételével. A tanulmányok zárásakor hozzájuk csatlakozott az előző évfolyamról további 1 hallgató, így eb-

²² Vezetői éves továbbképzés: jogi, közigazgatási, vezetéselméleti és szervezeti irányítási ismeretek, információbiztonsági technológiai ismeretek, informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek, közreműködői éves továbbképzés: információbiztonsági technológiai ismeretek, informatikai biztonságpolitikai, stratégiai, szabályozási ismeretek, jogi és szervezeti irányítási ismeretek.

ben a tanévben 26 szakdolgozat sikeres védeése történt meg. A szakdolgozatok közül 6 titkosításra került, jelenleg 20, korlátozás nélkül hozzáférhető szakdolgozat áll rendelkezésre az elemzéshez. A képzés harmadik évfolyama 2015 szeptemberében indult, 38 hallgatóval.

A szakdolgozatok szerzői a magyar közigazgatás (központi és területi államigazgatás, illetve önkormányzati igazgatás), valamint az Ibtv. által érintett piaci szféra különböző területeiről érkeztek, a dolgozatok tárgya is ennek megfelelő szóródást mutat.

A szakdolgozatok áttekintésének nem célja az egyes munkák tartalmának tételes értékelése, minősítése. A tanulmány – a hallgatók témaválasztása, a dolgozatokban megjelenő (régiből vagy újonnan megszerzett) tudásanyag legfontosabb elemeinek hangsúlyozottsága, a téma feldolgozásának módja, mélysége, valamint a felvetett általános és sok esetben konkrét problémák, kérdések alapján – az oktatói és a jogalkotói tevékenység tervezéséhez, végrehajtásához kíván – néhány szempont felvetésével – támogatást nyújtani.

A szakdolgozatok fent említett szempontok szerinti áttekintése alapján az alábbi megállapítások tehetők.²³

1. A szakdolgozatok – a hallgatók előképzettsége, munkaköre, érdeklődése alapján – részben informatikai-műszaki, részben jogi-igazgatási témákat tárgyalnak. A dolgozatok egy része a képzés során megismert tananyagokat, kapcsolódó szakirodalmat ismerteti, értékeli, másik része a megszerzett ismereteket és a saját, konkrét élményeket, problémákat, tervezett vagy már végrehajtott feladatokat írja le, veti össze. Mindkét típusban jelen vannak a „top témák”, a közkedvelt ábrák, szófordulatok.

2. Az Ibtv. és a 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményekről (a továbbiakban: technológiai rendelet) előírásainak teljesítésével összefüggésben jelentős az adminisztratív, szabályozási kötelezettségekkel kapcsolatos tartalom, így különösen az informatikai biztonságpolitika, informatikai biztonsági stratégia és informatikai biztonsági szabályzat, valamint a kapcsolódó eljárásrendek kidolgozása.²⁴ A szabályozás szintjeivel, tartalmával hat szakdolgozat foglalkozik.

Hangsúlyosan szerepelnek az informatikai rendszerekkel kapcsolatos besorolási, kockázatelemzési feladatok. Elméleti kérdéseket négy dolgozat tárgyal, három dolgozat saját módszertant ismertet, ugyanazon kockázatelemzési képletet két dolgozat idézi.

Külön kört képeznek az önkormányzatok, kis szervezetek esetében felmerülő problémák, különösen

- a saját információbiztonsági kapacitás, szaktudás hiánya;
- a biztonsági és üzemeltetési feladatok egy személy általi ellátása;

23 A közölt adatok arányokat, tendenciákat jelölnek, nem cél a teljes körű, tételes tartalomelemzés, felmérés.

24 2015. július 16-ai hatállyal a 77/2013. NFM rendelet helyébe lépett a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről. Az új jogszabály már nem tartalmazza az informatikai biztonságpolitika, informatikai biztonsági stratégia elkészítésére vonatkozó követelményt.

- az információbiztonsági feladatok ellátása kiszervezésének (outsourcing) szükségessége, terhei és kockázatai (kitettség, magas szakértői költségek stb.);
- a szolgáltatók által előkészített szerződések felelősséget korlátozó rendelkezéseinek diktátum jellege.

Figyelemre méltó a jogszabály végrehajtása során tapasztalt – a jogi szabályozás hiányoságaiból vagy éppen a túl szigorú szabályozásból fakadó – problémák köre. Ilyen például

- a más szervezet által fejlesztett és üzemeltetett informatikai („idegen”) rendszer használatának következtében felmerülő információvédelmi feladatok (pl. besorolás, kockázatértékelés szükségessége vagy a tulajdonos, szolgáltató általi értékelés átvételének lehetősége) és felelősségek tisztázatlansága;
- a központi és területi szervek, integrált és integrálódó szervezetek feladatellátása során felmerülő szabályozási, üzemeltetési és felelősségi kérdések, figyelemmel a többes és többszintű irányítási, felügyeleti jogkörökre, az elődszervezetek továbbelő eltérő gyakorlatára;
- a nagyszámú, eltérő infrastruktúrára működő, eltérő informatikai támogatással rendelkező alkalmazással összefüggő adminisztratív feladatok teljesíthetősége, ár-érték arányossága;
- az országos rendszerek, adatbázisok, hálózatok és ezek helyi részhalmozaira vonatkozó biztonsági elvárások teljesíthetősége központi, jelentősebb erőforrások és szűkös helyi erőforrások esetében.

Az előírt információvédelmi kötelezettségek és a forráshiány ellentéte szervezeti mérettől függetlenül megjelenik.

3. A felhasználók információbiztonsági közömbössége, az információbiztonsági tudatosság hiánya nyolc dolgozatban szerepel, a biztonságtudatosság növelését célzó oktatásról (tematika, tananyag, célcsoportok stb.) pedig hét dolgozat szól. Ezzel összefüggésben a kártékony kódok elleni védekezés szükségességével öt hallgató foglalkozott, a jelszóhasználatlal összefüggő hibákra (nem megfelelő hosszúságú, bonyolultságú jelszó használata, a jelszó felírása mások számára elérhető módon, közös jelszavak használata, jelszavak átadása stb.) hat dolgozatíró tért ki, a jogosultságkezeléssel és a felhasználói tevékenység naplózásával összefüggő problémákat három dolgozat tárgyalta.

4. A szakdolgozatok szakmai mélysége is változó. Egyes, erre egyébként is hajlamosító témáknál (biztonságtudatosság, kártékony kódok elleni védelem, jelszóhasználat, szabályozás) vélhetően az ismeretösszegzés, ismeretterjesztés volt a szerzők célja. Az ITB 12. ajánlásában szereplő adatbiztonsági ábrát öt, a PDCA²⁵ modellt két, a CIA²⁶ információbiztonsági elvet négy munka tartalmazza. Az esettanulmányok, a feladat-tervezések és -végrehajtások leírásai értelemeszerűen egyénibb látásmódot tükröznek, problémafelvetéseik konkrétabbak, életszerűbbek. A megkülönböztetés értékítéletet nem tartalmaz, mindkét típus szükséges és visszacsatolásként hasznosítható.

5. A jogi-igazgatási fogalomhasználat több dolgozatban pontatlan, hibás, elavult; előfordul már nem hatályos törvényre történő hivatkozás is.

6. Erős szóródást mutat a dolgozatok terjedelme.

25 PDCA: Plan, Do, Check, Act – Tervezés, Végrehajtás, Ellenőrzés, Beavatkozás

26 CIA: Confidentiality, Integrity, Availability – Bizalmasság, Sértetlenség, Rendelkezésre állás

7. A dolgozatok formai jellemzői kapcsán megjegyzendő, hogy több ízben előfordul szerkesztési következetlenség (mondatok, bekezdések ismétlése), központosási hiba, a hivatkozások jelölése nem egységes.

6. A KÉPZÉssel ÖSSZEFÜGGŐ ÉSZREVÉTELEK

A mottóban jelzett haszon több szempont szerint, több viszonylatban is értelmezhető. A hallgató új ismereteket szerez, új készségekre tesz szert, ezeket remélhetőleg hasznosítani tudja a napi feladatellátása kapcsán (a szakdolgozatok témaválasztásai utalnak arra, hogy a hallgatók és az oktatók is a gyakorlatban hasznosítható tudás megszerzését-átadását részesítik előnyben). A képzésen részt vett személyek a tudást tovább sugározzák munkahelyi környezetükben, így az Ibtv. hatálya alá tartozó szervezetek és munkatársaik másodlagos haszonélvezőivé válhatnak a képzésen átadott ismereteknek. Amennyiben az ilyen „haszonélvező” szervezetek száma növekszik, a jogalkotói cél – információbiztonsági szempontból megbízhatóbban működő információs rendszerek, tudatosabb felhasználók, biztonságosabb adatkezelés – is teljesülhet.²⁷

Ahhoz azonban, hogy ez az ismeretátadási rendszer folyamatosan biztosítsa a korszerű tudás terjesztését – részben az elvárások, részben a tapasztalatok alapján – a képzés folyamatos korrekciója, optimalizálása is szükséges.

A szakdolgozatok fent említett szempontok szerinti áttekintése alapján az alábbi megfontolások érdemelhetnek figyelmet.

1. Pontosítandó a képzés célja és ennek alapján a tartalma. Amennyiben a cél az információbiztonsági felvilágosítás, egységes szemlélet és gyakorlat elterjesztése, a „mindenből egy kicsit, rendszerezetten” elv – a korábbi képzések során teljesített tantárgyak alóli mentesítésekkel – érvényesülhet. Egy jogász számára a 10-20 órás, jogi ismeretek átadását célzó tárgy időpazarlás lehet, egy informatikus számára az információtechnológiai alapfogalmak „megismertetése” lehet felesleges. Ilyen tartalmú képzés elsősorban a biztonságtudatos szemléletmód kialakítását szolgálhatja; első körben a hallgatókét, ezt követően – amennyiben megszerzett ismereteiket továbbadják és ennek a tudástranszfernek kedvező a fogadtatása – a környezetükét. Amennyiben a cél a képzési rendeletben is megjelenített, piaci képzéssel egyenértékű szakmai kompetenciák átadása, a különböző előképzettséggel rendelkező hallgatók tananyagát differenciálni és mélyíteni kell műszaki-informatikai és jogi-igazgatási irányok szerint.

2. A fenti célok alapján célszerű az éves továbbképzést is újragondolni. Alapismerek évenkénti átadása nem túlságosan vonzó oktatási forma, magasabb szintű kurzusok biztosítása 3-5 évente rangot adó tapasztalatszerzés lehet.

3. A hallgatók előképzettségének különbözősége miatt a homogén oktatási csoportok és tananyag kialakítása nem feltétlenül célravezető (lásd előbb).

4. Az 1. és 2. pontban foglaltakkal összefüggésben kerülendő olyan ismeretek átadása személyes jelenléti képzésben, amelyek az arra feljogosított hatóság által kiadott ajánlásokban,

²⁷ SZÁDECZKY Tamás: *Information Security – Strategy, Codification and Awareness = ICT Driven Public Service Innovation: Comparative Approach Focusing on Hungary*, szerk. NEMESLAKI, Nemzeti Köszolgálati és Tanácsadó Kft., Budapest, 2014, 208, 109–122. (ISBN:978-615-5305-89-4)

útmutatókban is közzétehető, vagy kampányokkal közvetíthető (ez utóbbira példa lehet az Alkotmányvédelmi Hivatal Awareness programja).²⁸ A közigazgatásban ezek alapján egyes információvédelmi szakmai evidenciák az irányító, felügyelő szervek által kötelező normaként előírhatók, így a képzési időkeret mélyebb ismeretek átadására vagy az ismeretek elmélyültebb feldolgozására fordítható.

5. Az előző ponthoz is kapcsolódva célszerű lehet az egyénre szabottabb tanári támogatás (szükség esetén korrekció) biztosítása az előadásokon elhangzott tananyag feldolgozása és a szakdolgozat elkészítése során. A képzés akkor lehet sikeres, ha a közös „információvédelmi műveltségi minimum” biztosításán túl a hallgatóknak egyéni igényeiknek megfelelő szakmai felkészítést is nyújt, hiszen a végső cél olyan szakemberek képzése, akik a jogszabályokban előírt feladatokat végre tudják hajtani vagy hajtatni. Ehhez stabil, a mindennapokban alkalmazott tudás szükséges.

6. A mindennapokban alkalmazható tudás átadásának elvéhez kapcsolódva kifejezetten ajánlott konkrét segédletek, módszertanok megismertetése, kipróbáltatása. Így például hangsúlyos a jogszabályok által elvárt dokumentumok elkészítésének támogatása, de a feladatki-pipálás helyett a jogalkotói célnak megfelelő, valóban érdemi szabályozás és dokumentálás kialakításának támogatása szükséges.

7. Az oktatói felelősség érzékeny pontja a szakmai igényesség és az önkorlátozás egyensúlya megteremtésének megtanítása. A szakmai toposzok, közhelyek mechanikus ismétlése, a túlbuzgó lelkesedés (a dolgozatokban ezekre is akad példa) a várttal ellentétes hatást válthat ki. Az információbiztonsági szabályozás és felügyelet felhasználói élményt korlátozó tevékenységként jelenik meg a mindennapokban, nem kell a képviselőit még meg is utáltatni.

A megismert szakdolgozatok tartalmától független, de a megismerhetőséggel összefüggő javaslat a szakdolgozatok titkosításának mellőzése. Valóban érzékeny adatok felhasználásához a képzést finanszírozó szervek, szervezetek jellemzően nem járulnak hozzá (üzleti titkok, minősített adatok stb. felhasználása további védelmi garanciákat igényelne a képzést lebonyolító részéről). Ugyanakkor az általában kijelenthető, hogy a közigazgatási szervek foglalkoztatottjainak közpénzből finanszírozott képzésének eredménye legyen mindenki által hasznosítható tudás.

7. AZ IBTV. ÉS A KAPCSOLÓDÓ RENDELETEK VÉGREHAJTÁSÁNAK TÁMOGATÁSÁRA VONATKOZÓ JAVASLATOK

A szakdolgozatok témaválasztása, a kiemelten tárgyalt kérdéskörök, valamint a konkrét kérdésfelvetések, javaslatok egyértelműen utalnak azokra a problémákra, amelyek megoldásához a végrehajtásban érintettek további segítséget várnak.

1. A biztonsági besorolás (információs rendszer biztonsági osztályának, szervezet biztonsági szintjének a meghatározása) és a kockázatelemzés – előzmények híján – (túl) nagy feladatot jelent az Ibtv. hatálya alá tartozó közigazgatási szervek érintett munkatársainak. A kockázatelemzés megkönnyítéséhez célszerű lenne konkrét módszertani útmutató rendelkezésre bo-

28 Forrás: ah.gov.hu/html/awareness.html (2015. 10. 12.)

csátása, amely a képzésen oktató elméleti alapokon túl tartalmazhatná az előírt feladatok teljesítése során született eredményeket (amelyeket a jogszabály rendelkezése szerint a Nemzeti Elektronikus Információbiztonsági Hatóság számára meg kellett küldeni).²⁹ Az elektronikus információs rendszerek esetében felmerülő összes kockázat számbavétele, értékelése egységes gyakorlati útmutató nélkül aránytalanul nagy feladatot jelent az egyébként is kapacitáshiányos kis szervezeteknél (jellemzően önkormányzatoknál), ráadásul az eredmény szubjektív lesz, hiszen egyéni döntéseken múlik az egyes tényezők figyelembevétele.

2. A kis szervezetek már említett erőforráshiánya ismét többlemű probléma. Ha nincs információvédelmi szakember, külső szaktudást kell igénybe venni (a dolgozatok utalnak a 3–15 millió Ft-os áron ilyen jellegű szolgáltatásokat kínáló cégekre, illetve a kiszervezés információbiztonsági kockázataira is). Az outsourcing költségeire azonban nincs fedezet (ahogyan sok esetben az előírt információvédelmi eszközökre, megoldásokra sincs).

3. A jogszabályban meghatározott jelenlegi információbiztonsági elvárásrendszer – éppen a számonkérhetőség érdekében – nagyon kötött, szigorú; nem ad módot a szervezetek és információs rendszereik mérete, munkaszervezési sajátosságai szerinti differenciálásra, nem veszi figyelembe a különböző szervezetek által közösen használt, illetve a szervezetek együttműködő rendszereinek szabályozási és felügyeleti igényeit. A továbbiakban célszerű lenne megteremteni ennek lehetőségét.

4. Pénzügyi többletforrások biztosítása nélkül a jogszabályokban előírt feltételek teljesítésének lehetősége – még a két-két éves felkészülési időszakokkal is – erősen kérdéses.

5. Az információbiztonsági tudatosságra nevelés feladatának és felelősségének az információbiztonságért felelős személyre telepítése figyelmen kívül hagyja az előző pontokban jelzett erőforrásbeli problémákon túl azt a tényt is, hogy ennek a tevékenységnek a fogadtatása az érintettek részéről – részben a felhasználók hamis biztonságtudata miatt – az esetek túlnyomó többségében nem kedvező (az oktatás a szükséges rossz).

6. Ugyanez a helyzet az információbiztonságért felelős személy általános információbiztonsági feladatkörei tekintetében is. Nem elhanyagolható körülmény, hogy az információbiztonságért felelős személy csak egy a különböző szerveknél kijelölt számtalan felelős (adatvédelmi felelős, biztonsági vezető, integritás tanácsadó stb.) közül; nem mindenható, szervezeti presztízse és tevékenységének eredményessége másoktól, ez utóbbi nagymértékben a rendelkezésre álló pénzügyi erőforrásoktól is függ. Nem lehet cél sem a jogszabályi követelmények teljesítésének „lepapírozása”, sem az információbiztonságért magányosan küzdő „mártírok” kitermelése.

7. Szükséges lehet – a jelenlegi kinevezési és megbízási gyakorlatra tekintettel – az információbiztonságért felelős személy feladatellátáshoz szükséges végzettségére és szakképzettiségére vonatkozó rendelkezések korrekciója és ennek alapján a képzések, továbbképzések tartalmának finomhangolása.

29 Az Ibtv. módosítása eredményeként 2015. október 1-jén a Nemzeti Elektronikus Információbiztonsági Hatóság, a Kormányzati Eseménykezelő Központ (GovCERT) és a Nemzeti Biztonsági Felügyelet szervezeti keretén belül működő Cyber Defence Management Authority összeolvadásával megalakult a Nemzeti Kibervédelmi Intézet. Forrás: www.kormany.hu/hu/belugyminiszterium/rendeszeti-allamtitkarsag/hirek/megalakul-a-nemzeti-kibervedelmi-intezet

1. táblázat • A szakdolgozatok alapadatai

Cím	Tartalom
<i>Hatásköri kérdések az Ibtv. szabályozásában</i>	Az Ibtv.-ben meghatározott információvédelmi elvárások teljesítésével összefüggő kérdések a kormányhivatalok esetében, figyelemmel a kormányhivatalok és a központi hivatalok speciális kapcsolatára.
<i>Ágazati hitelesítés-szolgáltatás kialakítás IT biztonsági kérdései, különös tekintettel a fizikai biztonságra</i>	Az elektronikus aláírással kapcsolatos szolgáltatások létrehozásának feltételei, tervezésének folyamata, elvárt fizikai biztonsági környezete.
<i>Információbiztonsági kockázatok felmérése a Ceglédi Közös Önkormányzati Hivatalnál</i>	Kockázatelemzés elmélete és lehetséges módszertana egy konkrét önkormányzati szerv esetében.
<i>Biztonságtudatosságot fokozó oktatási program létrehozása a KÖTIVIZIG-nél</i>	Egy konkrét vízügyi szerv dokumentumkezelő rendszerének alkalmazása, alkalmassá tétele az információvédelmi dokumentumok kezelésére és hozzáférhetővé tételére, valamint a felhasználók információbiztonsági tudatosságát növelő audiovizuális oktatási anyagok készítése.
<i>Kormányzati célú elkülönült hírközlő hálózat információbiztonságának szabályozása</i>	A honvédelmi tárca információvédelmi szabályozásának bemutatása.
<i>Felhasználók biztonságtudatosságának kezelése</i>	Az informatikai biztonság fogalma, különös tekintettel az emberi kockázatokra (felhasználók, külső személyek tevékenysége). Az informatikai rendszerek felhasználóinak informatikai biztonsági tájékoztatása, képzése, biztonságtudatosságának növelése.
<i>Az Ibtv. implementálása kis szervezeteknél</i>	Az Ibtv. és végrehajtási rendeletei által meghatározott elvárások és feladatok az 1. és 2. biztonsági szintbe sorolt kisméretű szervezetek vonatkozásában.
<i>Biztonság fokozását szolgáló technikai eszközök kiválasztása</i>	Jogszabályok, stratégiák, szakmai ajánlások, módszertanok átfogó bemutatása az információbiztonsági tervezéssel összefüggésben.
<i>Ibtv. követelmények az egyszerű és összetett közgazgatási rendszerekben</i>	Az információvédelem szabályozási előzményei, az Ibtv.-ben meghatározott feladatok, felelőségek értelmezése, megvalósíthatóságának értékelése, az információbiztonsági tudatosság mérése.
<i>„Tudáscsöppek” – biztonság-tudatosító e-learning oktatás a XVIII. kerületi Polgármesteri Hivatalban</i>	Egy konkrét önkormányzati szervnél megvalósított információbiztonsági oktatás tartalma és tapasztalatai.

<i>A kiberbiztonság szerepének felértékelődése, mint napjaink fő biztonsági kihívása</i>	Elméleti összefoglaló, kibericidensek, szereplők összegző bemutatása.
<i>A felhasználók biztonságtudatosságának kezelése és fejlesztése az önkormányzatoknál</i>	Az információvédelem személyi aspektusai; helyzetértékelés és képzésre vonatkozó javaslatok egy konkrét önkormányzati szervnél szerzett tapasztalatok alapján.
<i>Adatvédelmi szempontból kiemelten veszélyeztetett objektumok biztonságtechnikai védelme</i>	Az információvédelem egyik részterülete: objektumvédelmi megoldások egy képzeletbeli nagykövetségi épület esetében.
<i>Felhasználók biztonságtudatosságának fejlesztése</i>	Az információvédelem különböző területeinek bemutatása. Kérdőíves felmérés a biztonságtudatosság növelését szolgáló oktatás előtt.
<i>A Csellömölki Közös Önkormányzati Hivatal információbiztonsági helyzete az Ibtv. tükrében</i>	Az Ibtv.-ből fakadó információvédelmi feladatok egy konkrét önkormányzati szerv esetében, különös tekintettel az elvárt alapidokumentumok elkészítésére.
<i>Az európai uniós pályázatkezelő rendszerek vizsgálata az elektronikus információbiztonsági vezető szemével</i>	Szoftverfejlesztés elméleti alapjai és biztonsági kérdései a Magyarországon alkalmazott pályázatkezelő rendszerekkel összefüggésben.
<i>Informatikai biztonságtudatosság-növelő oktatási anyag</i>	Biztonságtudatossággal kapcsolatos alapismeretek rendszerezése, példáulkkal, fogalommagyarázatokkal.
<i>A bírósági épületek komplex védelme napjaink biztonsági kihívásainak tükrében</i>	Egy elképzelt bírósági épület védelmi rendszerei (környezetbiztonság, vagyonvédelem, informatikai védelmi rendszer, személyalapú fenyegetések, adatközponttal szembeni elvárások).
<i>IBIR bevezetése a Zalavíz Zrt.-nél</i>	Információbiztonsági irányítási rendszer kiépítése a már működő és tanúsított minőségirányítási és környezetirányítási rendszerekhez történő illesztéssel.
<i>Humán kockázatok azonosítása és kezelése a közigazgatásban</i>	Az információbiztonsági felelősséget hordozó munkakörök szabályozási, oktatási kérdései, különös tekintettel a jogszabályok jelenlegi tartalmára és az elektronikus információbiztonsági vezető szakirányú továbbképzésre.

8. ÖSSZEGZÉS

Több, fent ismertetett dolgozat, számos előadás és tanulmány szögezi le, hogy az Ibtv. és végrehajtási rendeletei – beleértve a képzési rendeletet is – legnagyobb erénye, hogy megszülettek.

Egy-másfél évvel a hatálybalépésük után – figyelemmel az elmúlt időszak részben ismertetett történéseire – megállapítható, hogy jelentőségük ennél jóval összetettebb. Célokot tűztek ki és ezek megvalósításához támogató szervezeteket, folyamatokat rendeltek. Az első ered-

mények már megismerhetők. Annak érdekében, hogy a kitűzött célok és a megvalósítás érdekében megteendő lépések összhangja egyre nagyobb legyen, ahogyan az a képzés során is elhangzott, a visszacsatolások értékelése és a szükséges korrekciók sem maradhatnak el. Ehhez kívánt jelen tanulmány néhány felvetéssel hozzájárulni, remélhetőleg sikerrel.



SUMMARY IN ENGLISH: Information safety is a key factor today. Creating information security is a priority in public service. However, implementing and maintaining information security is not only a technical issue. The preparation and continuing education of administrative leaders as well as information managers are essential.

In 2014 the National University of Public Service launched a further training programme for information security experts. These trainings are required by the Act on Information Security of Hungary. This study summarizes the first experiences of the trainings, which is based on the students' final theses. The findings of this paper may serve as valuable feedback for the training organizers as well as for the legislator. This paper is based on the freely accessible final theses submitted in 2015.

Prof. Dr. Kovács László ezredes (kovacs.laszlo@uni-nke.hu): a Nemzeti Közszerződési Egyetem Hadtudományi és Honvédtisztképző Karának egyetemi tanára. Több mint húsz éve foglalkozik elektronikai hadviseléssel, valamint információs műveletekkel. Az egyetemen oktatóként részt vesz az alap-, mester- és doktori képzésben. Az oktatás mellett tudományos kutatásokat folytat, amelyek a kiberhadviselés, az információs terrorizmus, a kritikus információs infrastruktúrák védelme, valamint az információs hadviselés különböző kérdéseit vizsgálják. 2005-ben, illetve 2009-ben információs terrorizmus kutatási témával elnyerte a Magyar Tudományos Akadémia Bolyai János Kutatói Ösztöndíját. Több olyan PhD-hallgató tudományos témavezetője, akiknek kutatásai az információbiztonság, az információs támadások, illetve az ellenük való védekezés nemzetbiztonsági kérdéseit vizsgálják.

Nagyné dr. Takács Veronika (takacs.veronika@freemail.hu): szakokleveles külügyi szakértő, jogász. A Nemzeti Közszerződési Egyetem Katonai Műszaki Doktori Iskola hallgatója 2011 óta. Kutatási témája az adatvagyon-gazdálkodás a közigazgatásban: stratégiaalkotás és szabályozás a Nemzeti Adó- és Vámhivatal adatvagyon-gazdálkodási tapasztalatai alapján. Doktori kutatásai alatt közel 15 tudományos és szakkikke jelent meg a témában.

E-LEARNING-TANANYAGOK FEJLESZTÉSE A KÖZIGAZGATÁSBAN

A 2014 áprilisában elindult, megújult köztisztviselői továbbképzési rendszer a körülbelül 75 000 fős célcsoport számára jelentős mennyiségű kötelező képzést ír elő. A képzések nagy volumene, a résztvevők távolsága, és a költséghatékonyságra törekvés miatt az új továbbképzési rendszer egyik alapvető pillérét az e-learning képzések jelentik.

A Massive Open Online Course (MOOC) szolgáltató oldalak sikere megmutatta, hogyan lehet jelentős tömegeket hatékonyan tanítani e-learning-tananyagok felhasználásával úgy, hogy a képzés interaktivitása is megmaradhasson.

Ez inspirált minket, amikor a Nemzeti Közszerződési Egyetem ÁROP 2.2.19 projektjének keretein belül kifejlesztettük saját e-oktatási módszertanunkat, mely alapján összesen 100 komplex e-learning képzési programot készítettünk el. Cikkünkben bemutatjuk, milyen szempontok alapján választottuk képzéseinkhez a videós tananyagokat, és a projekt tervezésekor milyen előzetes fejlesztési folyamatot állítottunk fel. Ezután ismertetjük, hogyan valósult meg a fejlesztési folyamat a gyakorlatban. Az egyes lépések kapcsán megmutatjuk a főbb kockázatokat és a kritikus pontokat, illetve ezek kezelésének általunk azonosított lehetőségeit.

KULCSSZAVAK:

e-learning, fejlesztési folyamat, MOOC, oktatóvideó, továbbképzési rendszer, videós tananyag



1. BEVEZETÉS

2014-ben, többéves fejlesztés eredményeképpen elindult az új köztisztviselői továbbképzési rendszer. Az új rendszer fontos pillérei a képzéstervezés, kötelező továbbképzések és kreditpontok gyűjtése. A továbbképzési rendszerben 75 000 tisztviselő vesz részt, akiknek lakóhelye, korcsoportja, iskolai végzettsége vagy éppen munkaköre alapján a rendszer országos lefedettségű. Egy ilyen rendszer kifejlesztése és üzemeltetése képzésszervezés és tudásmenedzsment oldalról is óriási kihívás, melynek megvalósítása ekkora volumenben elképzelhetetlen az elektronikus képzési módszerekre való támaszkodás nélkül.

A Nemzeti Közszerződési Egyetem a képzések megvalósítását ezért jelentős e-learning-támogatással kívánta és kívánja megvalósítani. Az ezt támogatni hivatott ÁROP-2.2.19 „Elekt-

ronikus képzési és távoktatási anyagok készítése” című projektben komplex módszertani és technológiai fejlesztések valósultak meg, egy az egyetemen és a köztisztviselői képzésben egyaránt újnak számító e-tananyag-formátum került kifejlesztésre. A módszertan felhasználásával a projektben végül 100 képzési programban egyenként 4–7 e-learning-tananyag készült, melyből a 75 000 tisztviselő tanul és vizsgázik. A nagyságrendjét tekintve világszinten is jelentős online továbbképzési rendszerben ma már havonta több ezren tesznek vizsgát.

Az e-learningre sokan főként mint költségcsökkentő tényező gondolnak. Kétségtelen, hogy a digitális technikák használata csökkentheti egy képzés költségeit, azonban egy jó e-learning-tananyag kifejlesztése több száz munkaóra lehet. Kellően nagy képzési volumen esetében – mint például jelen esetben – így is lehet költséghatékonyabb a jelenléti oktatásnál, véleményünk szerint viszont az e-learning képzési forma választásakor nem ez kell legyen az elsődleges szempont, hanem a tananyagok minősége és az azok által elérhető tudásbővítés, hatékonyságnövelés.

Cikkünkben bemutatjuk a rendszer kifejlesztésének folyamatát a nemzetközi gyakorlatoktól kezdve a tervezett és megvalósított fejlesztési folyamaton keresztül a továbbfejlesztési lehetőségekig. Célunk, hogy a volumenében és hatásában is jelentős rendszer fejlesztési folyamatának bemutatásán keresztül segítséget nyújthassunk a jövő fejlesztéseinek.

2. NEMZETKÖZI GYAKORLATOK, VIDEÓSTANANYAG-TRENDEK

Az általunk választott videós formátumhoz az inspirációt az online szabadegyetemek kurzusformái adták. A MOOC-ok (Massive Open Online Course) esetében a tudás alapvető átadása rövid, sok esetben interaktív videós formátumban zajlik, a megszerzett tudást pedig tesztek és kvízek segítségével ellenőrzik.

Az online elérhető, bárki által szabadon felvehető kurzusok új világát már nem szükséges bemutatni. A MOOC-ok, az online szabadegyetemek viharos gyorsasággal válnak egyre népszerűbbé. Az első ilyennek tekinthető kurzus még 2008-ban indult 2300 fővel a Manitobai Egyetemen,¹ az igazi áttörést pedig a nagy presztízsű amerikai egyetemek piacra lépése hozta el. Elsősorban az edX platformot nonprofit formában működtető MIT és Harvard, illetve a Coursera kiinduló bázisát jelentő Stanford bejelentkezésével. Manapság a 2012-ben alapított, legnagyobbak számító online kurzusszolgáltató, a Courserán már közel 12 millió regisztrált felhasználó választhat az oldalon elérhető több mint ezer kurzusból. Világviszonylatban pedig több tucat szolgáltató versenyez a tanulni vágyó közönségért, melyeken keresztül 2014-ben 200%-kal nőtt az elérhető kurzusok száma.² Az első nem amerikai szolgáltató, amely elérte az 1 milliós felhasználói tábor, a spanyolajkúakra fókuszáló MiriadaX, de a legnagyobbak között említhetjük még a fenti példákon túl a Canvas Networkot vagy a FutureLearn szolgáltatót. A három legnépszerűbb kurzuskategória sorrendben: bölcsészet-

1 EDUCAUSE: *7 things you should know about...* MOOCs, 2011. Forrás: net.educause.edu/ir/library/pdf/eli7078.pdf (2015. 04. 28.)

2 A. HAYTOVA: *Global review maps the state of MOOC in 2014*, ICEF Monitor, 2015. Forrás: monitor.icef.com/2015/01/global-review-maps-state-moocs-2014/ (2015. 04. 28.)

tudomány, számítástechnika és programozás, üzleti tanulmányok.³ A legnépszerűbb kurzusok között megtalálhatunk mesterséges intelligenciával, az új vállalkozások indításával, programozással és a modern kortárs költéssel foglalkozó kurzusokat.⁴

A nagy felhasználószám és népszerűség mellett az elmúlt években már komoly jövedelmezőség is jellemzi a nagy oldalakat. A Coursera 2014-ben havi 1 millió dolláros bevételt realizált a tanúsítványok értékesítéséből.⁵ Felhasználói oldalról egyre komolyabb igény jelentkezik a „mini diplomának” tekinthető, kurzusok sorozatából álló képzések iránt, amelyek jelenleg kísérleti fázisban zajlanak több szolgáltatónál, pl. a Georgiai Technológiai Egyetemen. Egy másik ígéretes fejlesztési irány a „capstone” projekt keretében bevezetett, specializációs gyakorlati elem. A projektben részt vevő tanulók a tanúsítványok megszerzése után vállalatoknál tölthetnek el gyakorlati időt, ami ugyancsak a képzés része.⁶ Az új trendekbe illeszkedik a Udacity nanoDegree modellje, amelyben vezető IT-cégekkel együtt készített kurzusokat és feladatokat végezhetnek el havi díj ellenében a felhasználók. Ezek a képzések elsősorban az egyetemi képzéseket kiegészítő IT-ismeretek újszerű bemutatására fókuszálnak.⁷ A Udacityt alapító Sebastian Thrun azt jósolta, hogy 50 éven belül 10 intézmény fogja világviszonylatban biztosítani a felsőoktatást.⁸ Thrun azóta csökkentette elvárásait, és például a vállalati tréningek irányába fordította a Udacity üzleti elképzeléseit is. Egy másik komoly, általános problémája az online szabadegyetemnek az igen nagyszámú, 90% feletti lemorzsolódás. A MOOC-ok jövőjét illetően a nagyobb egyéni testreszabhatóság (automatizmusok által) az egyik fontos cél, illetve az, hogy az egyetemek megtanulják használni ezeket a platformokat, és egyszerre érjenek el sok hallgatót, de közben biztosítsák az egyéni fejlődési irányokat.⁹ A komolyabb egyéni haladás igénye és a valódi nyitottság igen fontos a MOOC felhasználók számára, az idei évben már számos igényalapú (on-demand) kurzus indul, amelyek esetében nem az ismert szemeszter logika érvényesül, hanem a tanulók egyéni tanulási tempója. Ebben komoly tényezők lehetnek a nagy amerikai egyetemek, ahol most „próbálgatják” kevert formában együtt kezelni az egyelőre elsősorban kiegészítő funkciót jelentő MOOC kurzusokat, saját hagyományos kurzusaikkal.¹⁰

A felhasználók komoly érdeklődése mellett a kurzusok készítői számára is új kihívást jelent a tartalmilag és technikailag is minél magasabb színvonalú kurzusok fejlesztése. Az edX

3 D. SHAH: *Online Courses Raise Their Game: A Review of MOOC Stats and Trends in 2014*, Class Central, 2014. Forrás: www.class-central.com/report/moocs-stats-and-trends-2014/ (2015. 04. 27.)

4 Online Schools Center: *Most Popular MOOCs by Category* – 2015. Forrás: <http://www.onlineschoolscenter.com/most-popular-moocs-by-category-2015/> (2015. 04. 28.)

5 SHAH: *How Does Coursera Make Money?*, edSurge, 2014. Forrás: www.edsurge.com/n/2014-10-15-how-does-coursera-make-money (2015. 04. 26.)

6 F. LARDINOIS (2015): *Coursera Partners With Google*, Instagram, 500 Startups And Others On Students' Capstone Projects, Techcrunch, 2015. Forrás: techcrunch.com/2015/02/11/coursera-partners-with-google-instagram-500-startups-and-others-on-students-capstone-projects/ (2015. 04. 26.)

7 Udacity.com: *Nanodegree*, 2014. Forrás: www.udacity.com/nanodegree (2015. 04. 25.)

8 S. LECKART: *The Stanford education experiment could change higher learning forever*, Wired, 2012. Forrás: www.wired.com/2012/03/ff_ai/class/ (2015. 04. 25.)

9 J. POPE: *What Are MOOCs Good For?*, MIT Technology Review, 2014. Forrás: www.technologyreview.com/review/533406/what-are-moocs-good-for/ (2014. 04. 28.)

10 SHAH: *Online Courses Raise Their Game: A Review of MOOC Stats and Trends in 2014*, Class Central, 2014. Forrás: www.class-central.com/report/moocs-stats-and-trends-2014/ (2015. 04. 27.)

esetében a Harvard egy több mint 50 fős produkciós stúdiót tart, de a Courserán is egyre komolyabb videós tartalmakon dolgoznak profi televíziós szakemberek bevonásával.¹¹ A Leideni Egyetem Coursera kurzusa 6 hónapig készült és 45 nap munkaterhelést jelentett az oktatónak, aki „mögött” folyamatosan dolgozott még egy tanársegéd is. A megjelenéshez a támogatást az egyetem online oktatólaborja támogatta videókészítésben jártas szakember, vágó, e-learning-módszertani szakértő, projektvezető és médiatréner segítségével. A Bostoni Egyetem a MOOC kurzusok készítését a mozifilmek forgatásához hasonlítja, egyfelől a résztvevő szakértők széles köre miatt, másfelől a tervezési és kivitelezési munkák összetettsége miatt. Esetükben is támogatja az oktatót egy tanársegéd, ő biztosítja a tematikát, az oktatási tartalmat, az alapul szolgáló írott, audio- és videotartalmakat, a feladatok leírását. Őket támogatja egy koordinátor, és egy e-learning-szakértő csapat, akik az első kapavágástól a kurzus lezárásáig biztosítják a módszertani és technológiai szaktudást. Felügyelik a kurzus lefolyását és értékelik azt, támogatják a marketinget. Ők biztosítják a kapcsolatot a technológiai és médiszakemberekkel, kapcsolatot tartanak jogi és adminisztratív kérdésekben, például az edX platform fejlesztőivel. A Bostoni Egyetem általános leírása szerint az első alkalommal 2-3 teljes szemeszternyi időráfordítást igényel az oktatók részéről a MOOC kurzus összeállítására 4-6 hónapos időtáv alatt. A videós tartalmak esetében maximum 5-10 perces videós előadások elkészítése a cél. Körülbelül 90 percnyi „hagyományos” kurzusanyag 30 percnyi MOOC videoanyagnak feleltethető meg.¹² A Barcelonai Egyetemen 10-15 perc a kitűzött videohosszúság, itt az amerikai egyetemekhez képest egyszerűbb technikai körülmények között készítik a kurzusokat. Jellemzően az oktatók saját maguk rögzítik a videós tartalmat, melyen osztott képernyőn jelenik meg a prezentáció és az oktató. A feliratot a Coursera biztosítja számukra, a kérdéseket pedig az oktatók időzíthetik. Az egyetem számítástechnikai eszközöket, illetve technikai csapatot biztosít a videók utómunkálataihoz.¹³

Az MTI kutatói közel 7 millió videós tartalmat átvizsgálva¹⁴ az alábbi megállapításokra jutottak a tanulók figyelmét illetően:

- A videók legyenek rövidek. Ne legyenek rövidebbek 6 percnél, de a készítők vegyék figyelembe, hogy a 9. perc után a figyelem elkezd csökkenni, és a 20. perc után az „internet nyer”, vagyis a felhasználók elkezdnek mással foglalkozni.
- Leginkább a 12 percnél hosszabb videók esetében figyelhető meg, hogy a tanulók jobban szeretik az informális hangulatú felvételeket, ahol az oktató például a saját irodája asztala mögött ül, mint amikor profi stúdiókörülmények között látható. A kutatók meglátása szerint a videó így sokkal inkább egyéninek, csak az adott tanuló számára készítettnek tűnik.

11 UL – Universiteit Leiden: *Leiden Online Learning Lab*, Mooc Studio, 2015. Forrás: leidenuniv.onlinelearninglab.org/mooc-studio.html (2015. 04. 27.)

12 DLI – Digital Learning Initiative: *How we produce MOOCs at BU*, Boston University, 2015. www.bu.edu/dli/how-we-produce-moocs-at-bu/

13 UAB – Universitat Autònoma de Barcelona: *Production and video editing*, 2015. Forrás: www.uab.cat/web/study-abroad/mooc/create-a-mooc/production-and-video-editing-1345668290962.html (2015. 04. 28.)

14 P. J. GUO, J. KIM, R. RUBIN: *How Video Production Affects Student Engagement: An Empirical Study of MOOC Videos*, 2014. Forrás: pgbovine.net/publications/edX-MOOC-video-production-and-engagement_LAS-2014.pdf (2015. 04. 28.)

- A tanulók szeretik a különböző előadás-technikákat keverő megoldásokat. Ezek lehetnek: „beszélő fejek”, élő kurzusokról felvétel, narrált prezentációk (jellemzően PowerPoint), képernyővideók, vagy Khan Academy stílusú videók hangalámondással, írással és rajzokkal. A kizárólag tantermi felvételeket kínáló videókat egyáltalán nem nézik a tanulni vágyók.
- A tanulók az előadásokat általában egyszer nézik meg, míg a támogató videókat többször is. Érdekes a támogató videókat könyvjelzőkkel kiegészíteni, hiszen a tanulók ugyan rövidebb, 2-3 perces etapokra, de gyakrabban visszatérnek.
- Nyilvánvaló megállapításnak tűnik, de a lelkesebb(nek tűnő) vagy energikusabb(nak tűnő) előadók kedveltebbek. Az már kevésbé nyilvánvaló, hogy ezt a hatást jellemzően az oktatók gyorsabb beszéde biztosítja.
- Másfélszer vagy akár kétszer annyi ideig figyelnek a tanulók azokra az oktatókra, akik az előadás közben írtak (kézírással vagy annak tűnő írással) vagy rajzoltak digitális táblára, mint ha csak a prezentációjukat narrálták volna. Így sokkal dinamikusabbnak tűnik a tartalom.¹⁵ A nemzetközi példák vizsgálata során tapasztalt pozitív gyakorlatokat saját videó formátumunk és tartalmaink fejlesztésénél is igyekeztünk maximálisan figyelembe venni, természetesen – ahogy azt a későbbi részekben megmutatjuk – a projekt külső és belső korlátainak, lehetőségeinek (például a rövid határidő, és rengeteg fejlesztendő videó, hogy csak a legfontosabbakat említsük) figyelembevételével.

3. FEJLESZTÉSI FOLYAMAT

Ebben a fejezetben bemutatjuk, milyen folyamat szerint terveztük elvégezni a videós e-tananyagok fejlesztését a projekt indulásakor. Az általunk felállított fejlesztési folyamat véleményünk szerint nemcsak a vizsgált projektben, hanem számos más e-learning-tananyagfejlesztésben is felhasználható, továbbfejleszhető. A fejezet alapjául a projekt megvalósíthatósági tanulmánya szolgál.

3.1. Képzési igények beérkezése

A folyamat első lépése a képzési igény megfogalmazása és továbbítása a fejlesztésekhez felállított e-learning-tananyagfejlesztő (projekt)szervezet (továbbiakban tananyagfejlesztők) felé. A szervezetet úgy kell felépíteni, hogy munkatársai között módszertani és technológiai tananyagfejlesztő szakemberek, tananyagszerkesztők, multimédiás szakemberek, gyártásvezetők és projektmenedzserek egyaránt megtalálhatók legyenek.

15 GUO: *How MOOC Video Production Affects Student Engagement*, 2014. Forrás: pgbovine.net/edX-video-production-research.htm (2015. 04. 28.)

B. NIELSON: *New Technologies Making MOOCs Even Better. Your Training Edge*, 2014. Forrás: www.yourtrainingedge.com/new-technologies-making-moocs-even-better/ (2015. 04. 28.)

L. LANDRY: *MIT-Spun 'YouTube for MOOCs' is Solving a Major Problem Plaguuing Online Education*, 2014. Forrás: bostinno.streetwise.co/2014/07/31/how-do-online-learners-watch-videos-lecturescape-mits-youtube-for-moocs-516442/ (2015. 04. 28.)

3.2. Igényfelmérés a célcsoport körében

AC-interjú és fókuszcsoportos kvalitatív módszerek segítségével felmérések elvégzése adott képzési program célcsoportjának tudás- és kompetenciaszintjéről, valamint attitűdjéről. A felmérés célja az igényekhez minél inkább testre szabott megoldások, tartalmak fejlesztése, a tanulási motiváció felkeltése és fenntartása.

3.3. Követelményspecifikáció

Ebben a lépésben a beérkező képzési igények alapján a tananyagfejlesztők módszertani csapata elkészíti a képzési programalapító és programfejlesztési dokumentumot (képzési PAD), amely többek között tartalmazza a képzési kimeneti követelményeket, a képzési célcsoportot, az erőforrásigényeket, a fejlesztés ütemezését és határidőit, illetve az egyéb specifikációkat (pl. szükséges-e fókuszcsoportos validálás a tananyagfejlesztéshez). A képzési PAD-ot a Programirányító Bizottság (PIB) fogadja el, amely egyaránt tartalmaz pedagógiai/didaktikai szakértőt, technológiai szakértőt/gyártásvezetőt, képzésszervező koordinátort, szakterületi felelőst (általában külső megbízott) és a projekt menedzserét is.

3.4. E-tananyag-szerzők kiválasztása

A képzési PAD alapján a projektmenedzsment lebonyolítja a szerzők kiválasztását, vagyis gondoskodik a szakértői pályázatok kiírásáról, a megfelelő szerzők kiválasztásáról, valamint lebonyolítja a szerzőkkel való szerződés-kötést.

3.5. Módszertani felkészítés

A szerzők/forgatókönyvírók módszertani felkészítése egy 2×6 órás workshop keretében történik meg. A felkészítőt a módszertani csapat szervezi és tartja meg, tematikája:

1. nap – általános felkészítő: alap forgatókönyvsablon kitöltésének mikéntje, alapszabályok, szerkesztési keretek, lehetőségek.

Az 1. nap után minden szerző önállóan elkészíti az adott tananyagra vonatkozó ontológiai térképet, amely a tananyag kifejlesztésére vonatkozó, az egyes lépéseket, összefüggéseket jelölő tervezési dokumentum.

2. nap – interaktív szakmai fórum: konzultáció a tananyagszerzőkkel, mely során a szerzőknek lehetősége van megvitatni az ontológiai térképet a fejlesztőcsapat részéről a pedagógiai/didaktikai, illetve a technológiai/IT-szakértőkkel, valamint a szakértők további tanácsokkal, javaslatokkal látják el a szerzőket.

3.6. Forgatókönyvsablon testreszabása

A módszertani felkészítő terméke az érintett tananyagokra vonatkozó forgatókönyvsablon, mely az alapformátumon, alapelvárásokon túl tartalmazza a szerző tananyag-specifikus ötleteit, javaslatait is.

3.7. Forgatókönyv készítése

A forgatókönyvsablon alapján a szerzők elkészítik az adott e-tananyagra vonatkozó forgatókönyvet. A forgatókönyvírás során a tananyagfejlesztők folyamatos didaktikai, módszertani, valamint technológiai és IT-szakértői támogatást nyújtanak a szerzőknek.

3.8. Forgatókönyv validálása, gyártási terv elkészítése

Az elkészült forgatókönyv szakmai validálását szakterületi lektor, módszertani validálását a tananyagfejlesztők módszertani munkatársai végzik. A forgatókönyvet nyelvhelyességi szempontból nyelvi lektor ellenőrzi. A tananyagfejlesztő csapat gyártási tervet készít a tananyaghoz, amely technológiai és IT szempontból ad meg specifikációkat a gyártó számára. A gyártási terv továbbá iránymutatást tartalmaz arra vonatkozóan, hogy a tananyaggyártás mely elemét lehetséges megoldani belső erőforrások felhasználásával, és mely elemek gyártását szükséges kiszervezni.

3.9. Munkamegrendelés

A gyártási terv alapján szükség esetén a projektmenedzsment csapat rendeli meg a kiszervezett feladatokat a külső szállító cégektől. Az erőforrások tervezésekor figyelembe veendő szempont, hogy meglehetősen nehezen tervezhető a gyártás ütemezése, illetve egy időben több tananyag gyártási folyamata összetorlódhat. Ezért a rendelkezésre állás rugalmasságának biztosítása érdekében érdemes lehet több szállító céggel keretmegállapodást kötni, így gyártási csúcs idején is garantálható a kiszervezett gyártási feladatok gyors és hatékony kivitelezése.

3.10. E-tananyag gyártása, illetve technológiai tesztelése

A gyártási folyamatot a gyártási tervben meghatározottak értelmében a belső tananyag-fejlesztői csapat és/vagy külső szállítók végzik. A tananyagfejlesztők részéről minden esetben a technológiai szakértő/gyártásvezető koordinálja a gyártás folyamatát.

3.11. E-tananyag validálása, visszaellenőrzés

Az elkészült tananyag validálása fókuszcsoportos tesztelés keretében történik, mely során a későbbi felhasználók csoportos interjú keretében direkt visszajelzést biztosítanak az e-tananyag tartalmával, kezelhetőségével, hatékonyságával kapcsolatban. Az e-tananyagra vonatkozó végső jóváhagyó döntés meghozatalára a PIB jogosult.

3.12. Kurzus kialakítása, kurzusmenedzsment

A kurzus az az e-learning-rendszer által biztosított felület, ahonnan a tananyag elérhető a tanulóknak, és ahol emellett számtalan kiegészítő lehetőséget találnak mind tartalmi (fogalomtár, videogyűjtemény, linkgyűjtemény stb.), mind kommunikációs (fórum, csevegőszoba, üzenetküldési lehetőség, blog stb.), mind pedig értékelési (leadandó feladatok, gyakorló- és vizsgatesztek, pontozás) szempontból. A tananyagoktól eltérően a kurzus nagyon gyors, az oktatás fajtájától függően akár napi szintű frissítéseket és ellenőrzéseket követel meg az oktatóktól. A kurzusmenedzsment keretében a technológiai szakértő/gyártásvezető kialakítja ezt a felületet (betölti az elkészült és validált e-tananyagot, létrehozza az egyéb tartalmi, kommunikációs és értékelési elemeket), majd a későbbiekben a tutorok folyamatosan frissítik és karbantartják (megválaszolják a tanulói üzeneteket, értékeli a teljesítményüket stb.) azt.

3.13. Toborzás a képzésre, a képzés lebonyolítása, hatásvizsgálat-elemzés

Végezetül a képzés szervezője tanulókat toboroz az elkészült képzésre, és a tutorok közreműködésével lebonyolítja a képzést. A képzés hatásvizsgálat-elemzése a tananyagfejlesztő és az eredeti képzési igény gazdájának közös feladata, mely történhet például az e-learning-keretrendszer statisztikái, elégedettségmérő kérdőív, tudásszintmérő tesztek vagy etnográfiai interjúk segítségével.

4. A TANANYAG FELÉPÍTÉSE

Az előzőekben ismertetett fejlesztési folyamatból a 3.3-as követelményspecifikáció pont a vizsgált projekt esetében abban különleges volt, hogy viszonylag szűk idő alatt (kevesebb mint 8 hónap) kellett viszonylag sok tananyagot (kb. 600 videót) fejlesztenünk. A nemzetközi gyakorlatoknál is említett időigényhez képest ez jelentős terhelést jelent, így olyan speciális tananyag kifejlesztésére volt szükség, amely egyszerre felel meg két szempontnak:

- rendelkezik egy olyan univerzális kerettel (tananyagmotor), amelybe viszonylag egyszerűen betölthetők a kész komponensek (jegyzet, ppt, videók) és előállítható a kész tananyag,
- a komponensek betöltése (gyártás) minél nagyobb részben automatizálható, így csökkentve a gyártás munkaigényét.

A kifejlesztett tananyagmotor felépítését az *1. ábra* mutatja be, a legfontosabb funkciókat is ismertetjük röviden, de a teljes struktúra működés közben megtekinthető a következő linken (https://probono.uni-nke.hu/upload/help/tutorials/ilias_tutorial.mp4) található – egyébként a képzés tanulóinak szóló – bemutató videóban is.

1. ábra • A tananyagmotor (Forrás: saját ábra)

NEMZETI KÖZSZOLGÁLATI EGYETEM A HAZAI SZÖVETSÉGBEN

keresés Q adatlap szakanyag fogalomtár letöltések segítség

A kiválasztástól a kinevezésig

A tananyag még nincs befejezve

A kiválasztás célja

- Célja: felkutatni a szervezet számára szükséges személyeket
- Kiválasztási stratégia meghatározása
- Függ:
 - a szervezet felépítésétől,
 - céljaitól,
 - a szervezeti kultúrától,
 - az anyagi erőforrásoktól,
 - a jogszabályi követelményektől,
 - a szakmai elvárásoktól.

01:45 / 37:46

világban, a versenyszerűen alapvetően a profitorientált, a minnél nagyobb profitot célzó szervezetek számára jelentős hasznót jelent, az a közszolgálatban természetesen nem jelentkezhet ilyen módon. Hiszen a közszolgálatban sokkal inkább a közfeladatok megfelelő ellátása, illetve, olyan ellátása lesz ez a hatékonyság mutató, ami alapvetően az ügyfél, az emberek, az állampolgárok elégedettségét, és a feladatok megfelelő elvégzését mutatja nekünk. Magában a közszolgálatban, közigazgatásban alapvetően nagy jelentősége van a

MAGYARI PROGRAM SZÉCHENYI TERV

ugrás a lap tetejére

5. ÖSSZEGZÉS

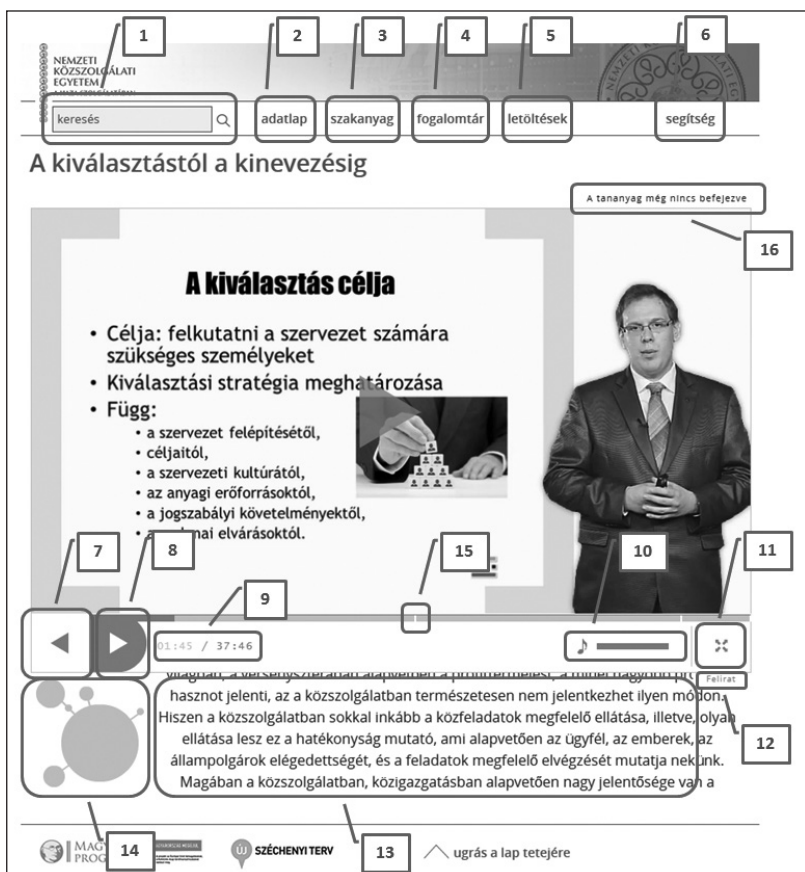
Cikkünkben bemutattunk néhány, a videós tananyagok és az azokat előszeretettel használó MOOC-ok kapcsán megjelenő fontos trendet, majd egy konkrét, megvalósult projekt vonatkozásában igyekeztünk a tananyagok fejlesztésének menetét bemutatni.

Az elkészült tananyagokkal és képzési rendszerrel kapcsolatban a visszajelzések kifejezetten pozitívak, amit többek között jól mutat, hogy az egyik tananyag a 2014-es INFOTÉR konferencián, az eFestival kiváló magyar tartalmak versenyen oktatás kategóriában az első helyen végzett.

Az, hogy a tananyagokból 75 000 ember tanul folyamatosan, természetesen kritikákat is eredményez. Ezek közül az egyik legfontosabb, hogy a tananyagokhoz felhasznált technológiák meghaladják sok tanuló munkaállomásának rendelkezésre álló lehetőségeit. Az általunk folyamatosan gyűjtött adatokból jól látszik, hogy ez a probléma arányaiban igen kis számú felhasználót érint, ugyanakkor a képzés kötelező jellege miatt az ő kritikáik is teljesen indokoltak

és érthetőek. Első körben ezt egyrészt a tananyagok letölthetővé és offline is lejátszhatóvá/elolvashatóvá tételével, másrészt a kötelező feltételek lazításával igyekeztünk orvosolni. Ezenfelül számos hosszú távú továbbfejlesztési lehetőség is látszik, mint például a Youtube vagy a szinte mindenhol rendelkezésre álló televíziókészülékek bevonása a tanulásba. A kifejlesztett tananyagmotor működését az alábbi ábra mutatja be.

2. ábra • A tananyagmotor menüpontjai (Forrás: saját ábra)



A fejlécben található a kereső és a tananyag menüpontjai.

1. **Kereső:** szabadszavas kereső, mivel az előadás videóként van rögzítve, így a felirat tartalmában keres. A legtöbb mai keresőhöz hasonlóan már gépelés közben mutatja a találatokat, jelölve, hogy a videóban hol (pp:mm) fordul elő az adott kulcsszó. Kattintásra a videó megfelelő részére ugrik.

2. **Adatlap:** a tananyaggal kapcsolatos legfontosabb adatokat jeleníti meg, mint a tananyag tárgya, nyelve(i), a képzési és kimeneti követelmények, tanulmányi előfeltételek, javasolt tanulási időtartam, vagy kötelező/ajánlott irodalom.

3. *Szakanyag*: a tananyaghoz tartozó tankönyv/jegyzet. Egységes előírások szerint tördelt dokumentum PDF formátumban, ami online, a tananyagon belül nyílik meg felugró ablakban.

4. *Fogalomtár*: a tananyaghoz tartozó legfontosabb fogalmak és magyarázataik listája táblázatos formátumban. A szakanyaghoz hasonlóan szintén felugró ablakban, de a tananyagon belül jelenik meg. Tartalmaz egy külön szabadszavas keresőt is, amely valós időben szűri a fogalmak listáját a keresett kifejezés szerint.

5. *Letöltések*: innen lehet letölteni a tananyaghoz tartozó szakanyag (tankönyv/jegyzet) PDF állományát, az előadáshoz tartozó diákat, a videó feliratát (TXT), hangsávját (MP3), vagy magát a videót (MP4). A tananyagok tervezésekor fontos alapelvünk volt, hogy a tanulók az összes építőelemet külön-külön is le tudják tölteni, és a tanulási stílusokhoz leginkább illeszkedő eszközön (e-könyv-olvasó, MP3-lejátszó, okostelefon stb.) tudják fogyasztani a tartalmat.

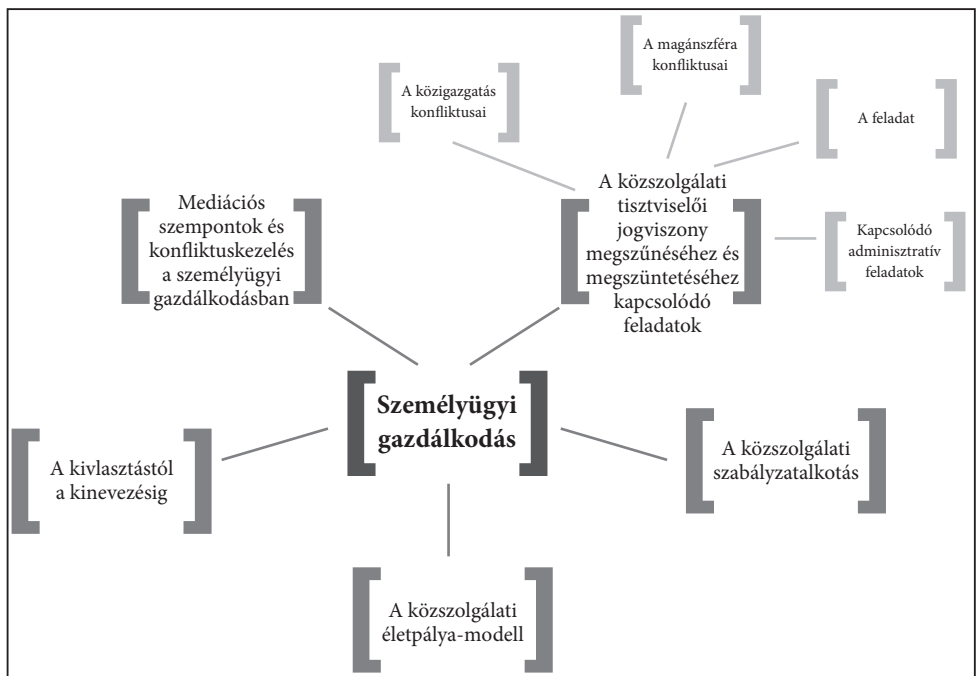
6. *Segítség*: megállítja a videó lejátszását, és megjelenít egy új réteget a tananyagban, ahol magyarázó szövegek és jelölések segítségével a konkrét videón magyarázzuk el a tanulónak az e-tananyag használatát.

A következő rész maga a lejátszó, ami a videókat megjeleníti.

Ez egyrészt az alapvető gombokat tartalmazza, mint: 7–8. *navigációs lehetőségek*, 9. *lejátszási idő*, 10. *hangerő-szabályozó*, 11. *teljes képernyős mód*, 12. *felirat ki-/bekapcsolása*, 13. *felirat megjelenítése*.

Másrészt olyan interaktív elemeket, amiket külön a tananyagmotorhoz terveztünk.

3. ábra • Egy képzési program tudástérképe (Forrás: saját ábra)



14. *Tudástérkép*: erre a gombra kattintva új ablakban nyílik meg a képzéshez tartozó tudástérkép. A központi fogalom a képzés címe, a második szinten található az egyes modulok (videók), majd azokból nyílnak az egyes diák, amelyek a videók háttérben szerepelnek. Az interaktív tudástérkép különböző színekkel jelöli a már megtekintett, illetve a még a tanuló előtt álló diákat és modulokat, valamint az adott anyagrészhöz navigálásra is használható.

15. *Ellenőrző kérdés(ek)*: a lejátszósávon található függőleges fehér vonalak jelölik a videót megszakító ellenőrző kérdéseket. A tananyag négyféle kérdést tartalmazhat, feleletválasztó (egy vagy több helyes válasz lehetséges), mondatkiegészítő, párosító vagy sorba rendező kérdéseket.

16. *Státuszbar*: a tananyagot az e-learning-rendszer akkor veszi elvégzettnek, ha a tanuló az összes kérdést megválaszolta. A tananyag állapotát (folyamatban/elvégzett) a státuszbarban jelenítjük meg. Ha a felhasználó erre a területre navigál a kurzorral, egyéb kiegészítő információkat is megjelenítünk a tanulási előrehaladás folyamatáról.



SUMMARY IN ENGLISH: The education system of the Hungarian public servants was renewed in April 2014. Online education plays significant role as 75.000 people are concerned. Popular Massive Open Online Courses (MOOC) offer a lot of video based study materials. The success of these courses inspired us at the National University of Public Services (NUPS) to develop about 100 video based e-learning courses.

We present a typical grouping of the different e-learning materials and the reasons behind choosing the video based methodology. We describe the planned development process and how it changed during the course of the project. In the article we are trying to show the pain points of the development and the risk management tools.

Orbán Zsolt (orban.zsolt@apertus.uni-nke.hu): a Nemzeti Közszerológati Egyetem tulajdonában álló Apertus Nonprofit Kft. e-learning-szakértője (e-learning-technológiai főreferens). Feladatai közé tartozik a fejlesztési projektek vezetése, módszertani felkészítők tartása, a tananyaggyártás koordinálása és új megoldások kutatása. Emellett a Budapesti Corvinus Egyetem Infokommunikációs Tanszékének PhD-hallgatója, kutatási területe az EU-s finanszírozású e-learning-projektek hatékonyságvizsgálata.

Balkányi Péter (balkanyi.peter@apertus.uni-nke.hu): a Nemzeti Közszerológati Egyetem tulajdonában álló Apertus Nonprofit Kft. e-learning-szakértője (e-learning-technológiai főreferens). Feladatai közé tartozik a fejlesztési projektek vezetése, módszertani felkészítők tartása, a tananyaggyártás koordinálása és új megoldások kutatása. Emellett a Budapesti Corvinus Egyetem Infokommunikációs Tanszékének PhD-hallgatója, kutatási területe a felsőoktatási e-learning-rendszerek adatbányászati eszközökkel történő vizsgálata.

A MAGYAR KÖZIGAZGATÁST KUTATÓK TUDOMÁNYOS LÁTHATÓSÁGA

Az alábbi cikkben a szerzők bemutatják a tudománymetria fogalmát, a tudományos teljesítmény mérőeszközeinek típusait, a tudományos láthatóságot biztosító eszközöket és a tudományos publikációk keresésének a módját. Továbbá megismerhetjük a magyar közigazgatással foglalkozó kutatók publikációinak számszerűsített mennyiségét, minőségét és hatását. Részletes ismertetésre kerül a korszerű kutatói közösségi médiák, Open Journal System és a repozitórium használata, ami együttesen javíthatja a kutatók tudományos láthatóságát.

KULCSSZAVAK:

h-index, impakt faktor, közigazgatás, közösségi média, open access, open journal system, repozitórium, tudománymetria, tudományos láthatóság



1. BEVEZETÉS

A minket körülvevő világ rohamosan változik.¹ Megváltoztak a publikálási, értékelési szokások, a lehetőségek, az előírások. Egyre fontosabb, hogy hol, mit, mennyit publikálunk, ki hivatkozik ezekre, milyen listákat tudunk megadni. Ezt kéri doktori értekezéseknél, habituszvizsgálatok során, pályázatok beadásakor. A világ Magyarországon és Európában is fokozatosan elcsúszik a formális, számszaki megítélés irányába.²

Manapság a kutatói életpálya minőségét is mérni lehet. Ennek egyik eszköze a *tudománymetria*, amely statisztikai módszerekkel méri a tudományos előrehaladást.³ Ilyen módon számszerűsíthetővé válik egy tudósnak a tudományterületére gyakorolt hatása, de munkájának minősége, mások általi elismertsége is összehasonlíthatóvá válik. Az

- 1 NEMESLAKI András: *Projekt menedzsment*, Aktuális Üzleti-Vezetési Szeminárium Sorozat; Nemzetközi Menedzser Központ, Budapest, 1995, 5, 88.
- 2 KOLLÁR István: *Tudományos publikálás hatékonyan, Hogyan publikáljunk, hogyan keressünk a szakirodalomban, hogyan mutassuk meg magunkat a weben, hogyan segítsük elő, hogy használják eredményeinket, és hogyan keressük meg a hivatkozásokat?* Gondolatok, információk doktoranduszaink (és kutatóink) számára, 2015. Forrás: oldweb.mit.bme.hu/services/pubinfo/szakirod-kezeles.pdf (2015.11.15.)
- 3 VINKLER Péter: *Tudománymetriai kutatások Magyarországon*, Magyar Tudomány, 2008/11, 1372–1380.

elismertségmérés leggyakoribb eszköze egy adott tudományos munka közvetlen idézettségének mennyiségi vizsgálata. Ehhez az interneten fellelhető adatbázisok nyújtanak segítséget. Ilyenek például: az ISI Web of Science, a Scopus, a Google Scholar vagy az MTMT. Manapság két mérőszámot használnak leginkább: az impakt faktort és a Hirsch-féle h-indexet. A fent említett adatbázisok egyúttal *tudományos láthatóságot* is biztosítanak, valamint gyorsabban összeköthetők olyan tudományos folyóiratokkal, amelyek rendelkeznek online kiadással is. A tudományos láthatóság fontos kérdés. Egy olyan tudományos folyóirat, amely nemzetközi ismertségre vágyik, illetve meg akarja magát méretetni más nemzetközi folyóiratokkal, nem kerülheti el az online térre való kilépést.

Napjainkban a tudományos és felsőoktatási intézmények kutatói számára egyre nagyobb jelentősége van annak, hogy a hálózatok világában mennyire látható az adott kutató és intézmény. Az Open Access (OA) mozgalmat, többek között, ez a jelenség indította el. Az OA filozófia középpontjában a tudományos cikkek, tanulmányok szabad elérhetősége állt.⁴

Ez a cikk megpróbálja bemutatni a tudománymetria fogalmát és tárgyát, majd a bemutatott mérőszámok segítségével felmérni a Pro Publico Bono korábbi szerzőinek tudományos teljesítményét és a tudományos teljesítményt támogató eszközök használatát.

2. A TUDOMÁNYMETRIA KIALAKULÁSA, TÁRGYA ÉS MÓDSZERE

Az a gondolat, hogy az egyes szakterületek irodalma ugyanolyan rendszeres kutatásnak vethető alá, közel 100 éves múltra tekinthet vissza.⁵ Cole és Eales mérte fel először, hogy a különböző kutatók hogyan járultak hozzá a korabeli tudományhoz.⁶ Ezt követően számos hasonló vizsgálatról szóló közlemény jelent meg, melyek más szakterületek tanulmányozására is kiterjedtek.^{7,8} Így a kialakuló új módszernek más, különböző elnevezései alakultak ki. Derek de Solla Price munkájában jutott kifejezésre először a tudomány mérésére, kvantifikálására (mennyiségi mutatókkal való jellemzésére, leírására) irányuló törekvés, amely a tudománymetria diszciplína (tudománymérés tudománya) kialakulásához vezetett.⁹ John M. Ziman ezt a tudománytörténet egyik legjelentősebb eseményének tekinti.¹⁰

4 DANI Erzsébet, BODA István: *Láthatóság, tudomány, Open Access – a tudományos eredmények láthatóságának vizsgálata a V4-ek országaiban*, 61/6, Tudományos és Műszaki Tájékoztatás, 2014. Forrás: tmt.omikk.bme.hu/show_news.html?id=5924&issue_id=560 (2015. 11. 15.)

5 BUJDOSÓ Ernő: *Bibliometria és tudománymetria*, OSZK, Budapest, 1986. Forrás: library.hungaricana.hu/hu/view/MTAKonyvtarKiadvanyai_OSZKMKK_1/?pg=215&layout=s (2015. 11. 15.)

6 FRANCIS JOSEPH COLE, NELLIE BARBARA EALES: *The history of comparative anatomy. Part I: A statistical analysis of the literature*, Science Progress, 1917/11, 578–596.

7 EDWARD WYNNDHAM HULME: *Statistical bibliography in relation to the growth of modern civilization: two lectures delivered in the University of Cambridge in May, 1922*, London, Butler & Tanner, 74.

8 JOHN DESMOND BERNAL: *The social function of science*, George Routledge, 1939, 482.

9 DEREK J. DE SOLLA PRICE: *Little Science Big Science*, Columbia University Press, 1963, 119.

10 JOHN MICHAEL ZIMAN: *Information, Communication, Knowledge*, Nature, 224318, 1969.

A *tudománymetria* azoknak a mennyiségi módszereknek az összessége, amelyek az információs folyamatként értelmezett tudomány vizsgálatával foglalkoznak.¹¹ Törvényszerűségei statisztikus érvényességűek. Ez azt jelenti, hogy minden tudományos eredmény a korábban lefektetett elvekre épül, az új tudományos eredmények a korábbiak újraértelmezése, továbbfejlesztése révén keletkeztek.¹²

A *tudománymetria* létrejöttének oka:¹³

Nő a tudományos publikációk száma. Több mint félmillió élő tudományos folyóirat van, a növekedés kétszereződési ideje tudományterülettől függően 5–15 év.

A tudomány termelési ágga válik, kialakul a *tudománypolitika*. A tudománypolitika a tudomány finanszírozását, a tudományos kutatások és azok által létrehozott technológiák szabályozását foglalja magában. A tudománypolitika fontos részét képezi a tudományos ösztönzők rendszerének koordinálása, melynek célja a magyar tudósok, kutatók tudásának szélesítése, a kutatói utánpótlás biztosítása, a kutatás-fejlesztés hatékonyságának növelése; valamint a tudomány népszerűsítése és képvisellete belföldön és külföldön egyaránt.

A tudományos alkotómunka egyik megnyilvánulása az új eredmények publikálása. A legismertebb tudománymetriai mérési eljárások a publikációk *mennyiségét, minőségét és hatását* próbálják meg számszerűsíteni.

Mivel a különböző jellegű művek munkaigénye és szerepe más és más, ezért ezt gyakran kategóriákba csoportosítva szokás megadni. Ilyen kategóriák például könyvek, könyvfejezetek, lektorált cikkek idegen nyelvű szakfolyóiratokban, lektorált cikkek magyar nyelvű szakfolyóiratokban, nem lektorált cikkek, térképek, digitális adathordozón megjelent művek, ismeretterjesztő cikkek, internetes cikkek stb.

A tudományok, különösen a társadalomtudományok művelőinek publikációs listáiban hagyományosan – legalábbis még néhány évtizeddel ezelőtt is – általában és természetesen első helyre kerültek az önálló tudományos könyvek:¹⁴

- az évtizedes kutatómunka eredményeit összegző monográfiák,
- az átfogó tematikájú tudományos szakkönyvek,
- a saját kutatási eredményeket is felölelő, a nemzetközi irodalom ismeretanyagát feldolgozó tankönyvek.

A tudományos teljesítmények értékelésében, illetve a tudomány művelőinek minősítésében – különösen a kutatások finanszírozásában –, a vonatkozó pályázatok elbírálásában újabban

11 NALIMOV Vasily Vasilevich, MUL'CHENKO, Z. M.: *Наукометрия, Изучение развития науки как информационного процесса*, Nauka, Moscow, 1969, 191.

12 JUHÁSZ Zsolt: *A katonák fizikai alkalmasság-vizsgálatával foglalkozó forrásmunkákról*, *Hadtudomány* 2009/1–2, 113–118. oldal. Forrás: mhtt.eu/hadtudomany/2009/1_2/113-118.pdf (2015. 11. 15.)

13 TAMÁS NÉ Fekete Adrienn: *Könyvtári ismeretek alapképzésben részt vevő hallgatóknak*, 2014. Forrás: eklektika.ekt.f.hu/sites/default/files/2014_konyvtari_ismeretek_alapkepzesben_resztvevo_hallgatoknak.pdf (2015. 11. 15.)

14 CSABA László, SZENTES Tamás, ZALAI Ernő: *Tudományos-e a tudománymérés? Megjegyzések a tudománymetria, az impakt faktor és az MTMT használatához*, *Magyar Tudomány*, 2014/4, 442–466. Forrás: www.matud.iif.hu/2014/04/12.htm (2015. 11. 15.)

világszerte markáns eltolódás tapasztalható a mennyiségi szemlélet irányába, valamint a tudományos könyvek rovására a folyóiratokban megjelent cikkek és hivatkozások javára.¹⁵

A kutatók számának folyamatos növekedésével és a kutatásra fordítható pénzek zsugorodásával nyilvánvalóvá vált, hogy a több száz éve többé-kevésbé eredményes „peer review”-féle értékelésen alapuló döntéshozatal egyedüli alkalmazása számos elvi és gyakorlati akadályba ütközik, és önmagában nem képes kielégíteni a modern korok értékelési igényeit.¹⁶

Egy publikáció jelentőségét azzal is becsülhetjük, ha megszámoljuk a forrásmunkaként rá hivatkozó más publikációkat. Hasonlóképpen, egy kutató munkájának jelentőségét kifejezheti az, hogy műveire összesen hány, mások által írott *hivatkozást* (citációt) kap.

Mind hazánkban, mind világszerte kb. a 60-as évektől kezdődően kerültek előtérbe az ún. kvantitatív értékelési eljárások, különösképpen azok, amelyek a szakirodalmi publikációs teljesítmény statisztikai elemzésére épülnek.¹⁷

Eugen Garfield 1963-ban egymással összemérhető folyóirat-jellemzőket dolgozott ki, s ezeket 1972 óta az Institute for Scientific Information (ISI) kiadványaiban közzéteszik. Ha egy folyóirat előző két évben megjelent cikkeire való hivatkozásainak számát elosztjuk az adott két évben e folyóiratban megjelent cikkek számával, egy arányszámot kapunk. Az így kapott értéket Garfield *hatástényezőnek* (impakt faktor) nevezte. Minél magasabb értéket kapunk egy folyóiratra az adott időintervallumban, annál „*hatásosabbnak*”, rangosabbnak számít a folyóirat, következésképpen egy kutató számára annál nagyobb dicsőség ebben a folyóiratban publikálni.¹⁸

Az első impaktfaktor-lista 1976-ban jelent meg, az 1975-ös Science Citation Index Journal Citation Reports (SCI JCR) kötetében. Az 1972–73-as cikkek 1974-es átlagos idézettségét adta meg. Magyarországon alkalmazták először ezt a listát, illetve az impakt faktort a tudományos teljesítmény értékelésére.¹⁹ Az IF tehát egyfajta átlagos hivatkozási szám az ISI által figyelt mintegy 6700 folyóirat körén belül. Összeadásuk nem is helyes, mert az IF-et csak folyóiratokhoz és nem cikkekhez rendeli, összehasonlításuk legfeljebb csak egy nagyon szűk szakterület kutatóinak összehasonlító értékelésére használható.²⁰ Előnye az egyéni idézettségre építő mutatókkal szemben, hogy súlyozza, hogy a szerzőt mennyire rangos folyóiratok idézik. A folyóiratok presztízsének mérésére az impakt faktor mellett több újabb alternatív mutató is megjelent:

15 CSABA-SZENTES-ZALAI: *i. m.*

16 BRAUN Tibor, SCHUBERT András: *Szakértői bírálat (peer review) a tudományos kutatásban*, Válogatott tanulmányok a téma szakirodalmából, MTA Könyvtára, Budapest, 1993, 200. Forrás: library.hungaricana.hu/hu/view/MTAKonyvtarKiadvanyai_INFORM_07/?pg=205&layout=s (2015. 11. 15.)

17 BRAUN Tibor: *Idézettség szövegkörnyezet-elemzés kutatók és kutatócsoportok teljesítményének értékelésére a nanoszerkezetek kutatásán bemutatva*, Magyar Tudomány, 2006/7, 862.

18 Eugene GARFIELD: *Citation Indexing Its Theory and Application in Science, Technology and Humanities*, John Wiley & Sons Inc., 1979, 296.

19 MARTON János: *Magyar publikációk külföldi folyóiratokban. Bibliometriai vizsgálatok az élettudományok területén*, Magyar Tudomány, 23. köt., 1978, 922–926.

20 KOLLÁR: *i. m.*, 10.

- *Eigenfactor* (EF): Jevin West és Carl Bergstrom a folyóiratcikkek olvasásával eltöltött idő alapján állít fel rangsort, mégpedig a Journal Citation Reports-ban (JCR) rögzített összes folyóirat arányában, az utolsó 5 év hivatkozásainak keresését figyelembe véve;²¹
- *Article Influence* (AI): az Eigenfactort kiegészíti a folyóiratokban megjelenő cikkek számának figyelembevételével;
- *SCImago Journal Rank* (SJR): az SJR a súlyozott idézetek átlagértékét mutatja adott évre vonatkozóan: az elmúlt 3 évre visszamenőleg vizsgálja a publikációk számát és az idézettséget is;²²
- *Source Normalized Impact per Paper* (SNIP): korrigálja az egyenlenségeket a különböző tudományterületek idézési szokásait, gyakoriságait figyelembe véve. Kidolgozása a Leideni Egyetem egyik kutatója, Henk Moed nevéhez fűződik;²³
- *Journal to Field Impact Score* (JFIS): ugyancsak tudományterületi hatást mér, de előre meghatározott tudományosztályozási rendszeren alapul, bázisa a Web of Science.

Az elmúlt években sokan rádöbbentek, hogy a szokásos indexek mennyire tökéletlenek, és ők most a közelmúltban bevezetett *Hirsch-index*től (h) remélik az előrelépést. (Egy szerző h-indexe 10, ha legalább tíz olyan publikációja van, amelyre legalább tíz hivatkozást kapott.)²⁴ Már Derek De Solla Price 1963-ban felhívta a figyelmet, hogy néhány területen a friss munkákra való hivatkozás aránya is csökkenhet.²⁵ Jelen szerzőnek számos harminc éven túl kapott idézete is van. Általában is igaz, hogy például a biológiában főként a nagyobb időtávlatban kialakuló citáltság lehet mérvadó, ezért az itt aktív kutatók joggal üdvözölhetik a h-index előtérbe kerülését. Hiszen amíg az impakt faktor a megjelenés évét követő két év citációinak, és csak az ISI-ben szereplő folyóiratok citációinak számából alakul ki, addig a h-index értékét valamennyi citáció, így az általunk legfontosabbnak tartott, szakkönyvekben kapott citációk is befolyásolják.²⁶

Természetesen egyetlen mutató, és így ez az index sem lehet mentes a torzításoktól, de nem lehet rezisztens a manipulatív szándékokkal szemben sem. Jorge E. Hirsch azt írja, hogy indexe nem érzékeny a függő citációk bevonására vagy kihagyására, és ezt konkrét esettanulmányai is alátámasztják.²⁷ Ez az index fontos, de meglehetősen részleges információt tartalmaz csupán, és több fogyatékosága is van, mint számításának módja, az idézetek, il-

21 Carl T. BERGSTROM, Jevin D. WEST, Marc A. WISEMAN: *The Eigenfactor™ Metrics*, Journal of Neuroscience, 28(2008)/45, 11433–11434. (DOI: 10,1523 / JNEUROSCI.0003-08.2008. PMID 18.987.179, 2008)

22 Borja GONZÁLEZ-PEREIRA, Vicente P. GUERRERO-BOTE, Félix MOYA-ANEGÓN: *A new approach to the metric of journals scientific prestige: The SJR indicator*, Journal, of Informetrics, 4(3), 379–391. Forrás: dx.doi.org/10.1016/j.joi.2010.03.002 (2015. 11. 15.)

23 Henk F. MOED: *Measuring contextual citation impact of scientific journals*, Journal of Informetrics, Vol. 4., Issue 3., July 2010, 265–277.

24 Jorge Eduardo HIRSCH: *An Index to Quantify an Individual's Scientific Research Output*, Proceedings of the National Academy of Sciences of the United States of America, 2015, 102, 46, 16569–16572.

25 DE SOLLA PRICE: *i. m.*

26 RÓZSA Lajos, PAPP László: *A csoportmunka mint egyéni érdem és egyéb megjegyzések, a köztestületi és publikációs adattár használatáról*, Magyar Tudomány, 2009/1. Forrás: www.matud.uif.hu/2009/09jan/16.html (2015. 11. 15.)

27 HIRSCH: *i. m.*, 4.

letve hivatkozások felmérésének szűk köre, időbeli korlátozottsága, a szakterületek közötti nagy különbségek figyelmen kívül hagyása, továbbá a cikkek és hivatkozások műfaji, tartalmi megkülönböztetésének hiánya, valamint és nem utolsósorban a cikkek szerzőinek számától való elvonatkoztatás miatt.

Leo Egghe 2006-ban a h-index továbbfejlesztéseként hozta létre a *g-indexet*. Abban különbözik a h-indextől, hogy az idézetek összegét nézi, vagyis g publikációnak összesen legalább g² (a bevont cikkek számának a kétszerese) idézete van.²⁸

Az i10-index azoknak a tanulmányoknak a száma, amelyekre egyenként legalább 10 hivatkozás történt.

A publish or perish szemlélet és a tudományos verseny nyomásának hatására a tudományos közlemények „rangsorában” első helyre kerülnek a folyóiratcikkek és más, időszaki, illetve elektronikus kiadványokban gyorsan publikálható írások. Nemcsak általában a hosszabb átfutású publikációk rovására, hanem különösen a lektorált szakkönyvek és az adott tudományág elért eredményeit kritikailag feldolgozó és saját kutatási eredményekkel kiegészítő egyetemi tankönyvek ellenében.²⁹

A tudományos érték mérőszámairól összességében elmondható, hogy nincsen egyetlen olyan mutató sem, ami önmagában minden szempontból megfelelő. Több szempont egyidejű figyelembevételével lehet csak értékelni egy szerző, egy folyóirat, egy intézmény, egy tudományterület vagy egy ország tudományos teljesítményét.

3. TUDOMÁNYOS LÁTHATÓSÁGOT SEGÍTŐ ESZKÖZÖK

Az információs szabadság létrejöttét támogató *open*, azaz nyílt kezdeményezések az elmúlt évtizedben jutottak el arra a szintre, hogy a tudományos kommunikációban komolyabb szerephez juthattak. Ezek legjelentősebbjei:³⁰

- az Open Source (nyílt forráskód),
- az Open Standards (nyílt szabványok),
- az *Open Access* (OA), vagyis a nyílt hozzáférés.

Amennyiben a publikáció hagyományos előfizetői modellt alkalmazó folyóiratban jelenik meg, a kiadók nagy része biztosít OA megváltást, mely a publikáció beküldésekor választható külön díj ellenében. Ebben az esetben a publikáció szabadon elérhető bárki számára a kiadó honlapján. A nyílt hozzáférés megváltási díjának kifizetése nélkül is van lehetőség előfizetői modellt alkalmazó folyóiratban megjelent publikációk nyílt hozzáféréseinek biztosítására, ez a szerzők önarchiválási lehetősége. Az egyes kiadók különféle módon szabályozzák

28 LEO EGGHE: *Theory and practise of the g-index*, Scientometrics, 2006, Vol. 69. No. 1., 131–152. (DOI: 10.1007/s11192-006-0144-7)

29 CSABA László, SZENTES Tamás, ZALAI Ernő: *Mégis, kinek az Akadémiája?* Magyar Tudomány, 2015/9, 1113–1137. Forrás: www.matud.iif.hu/2015/09/14.htm (2015.11.15.)

30 BARTON Dávid, PÁL Vanda: *Open access és osztályozás*, Könyvtári figyelő, 2013/4. Forrás: ki.oszk.hu/kf/2013/12/open-access-es-osztalyozas/ (2015. 11. 15.)

az önarchiválás lehetőségét, megkülönböztetve a publikációk különböző változatait, melyek a következők lehetnek:³¹

- *preprint*: ez a változat az első kézirat, melyet a szerző szakmai lektorálás céljából küld meg a kiadónak. (A preprint változat archiválása csak abban az esetben javasolt, ha a lektorálás után jelentős, tartalmat érintő változás nem történt!)
- *postprint*: az utolsó szakmai lektorálás utáni szerzői kézirat, ezt követően tartalmi változás a publikációban nem történik.
- *kiadói változat*: általában a kiadó honlapján megjelenő, szerkesztett, oldalszámmal és egyéb információkkal kiegészített változat.

Az önarchiválás azt jelenti, hogy a szerző a benyújtott publikációja bizonyos változatát (preprint, postprint, kiadói változat) esetleges megkötésekkel elhelyezheti az intézete által üzemeltetett repozitóriumban, amennyiben a kiadó engedélyezi. Az egyes kiadók, folyóiratok által biztosított lehetőségekről a Sherpa-ROMEÓ³² adatbázis ad irányadó információkat, jogilag természetesen a szerző kiadóval kötött szerződése a meghatározó, továbbá érdemes tanulmányozni a kiadó honlapját is.

Amennyiben a teljes szövegű változat elhelyezhető a repozitóriumban, a publikáció szabadon elérhetővé válik az olvasók számára, ami növeli a publikáció elérhetőségét más kutatók számára.

Az OA dokumentumokat különálló digitális könyvtárak, intézményi repozitóriumok őrzik, amelyeknek formai és tartalmi feltárása éppoly fontos, mint hagyományos társaiké.³³

A repozitórium egyetemeken és kutatási intézményekben működő dokumentumszerver, amely tudományos anyagok archiválására és világszerte díjmentes hozzáférhetővé tételére szolgál. Szakszerűen feltárja a feltöltött dokumentumokat, összekapcsolja a meglévő adatbázisokkal és egyben módot ad arra, hogy a különféle repozitóriumindexelő rendszerek a feltöltött anyagokat hatékonyan bekapcsolják a világ tudományos vérkeringésébe.³⁴

A repozitóriumok esetében alapfeltétel, hogy szemantikai szempontból megfelelően legyenek leírva a benne foglalt publikációk, lehetővé téve ezzel a közös keresők és az egyéb webet indexelő keresők (például Google, Google Scholar stb.) számára, hogy releváns találatokat adjanak.³⁵

A Magyarországon legelterjedtebb repozitóriumszoftverek, az EPrints és a DSpace nyílt forráskód alatt futnak, ami biztosítja a hosszú távú fejlesztés lehetőségét.

A közösségi médiát sokan olyan eszközként üdvözlik, mint amely a tudományos kommunikáció területén új és hatékony eszközöket kínál a tudás megtalálásához és megosztásához.³⁶

31 Open Access – Önarchiválás intézeti repozitóriumba. Forrás: lib.semmelweis.hu/nav/open_access_onarchivalas (2015. 12. 01.)

32 Pontos elérés: www.sherpa.ac.uk/romeo/index.php?la=hu

33 HOLL András, HARANGI Gabriella, DRÓTOS László, HOFFMANN Ádám: *MTMT rendszerrel együttműködő repozitóriumok minőségének ajánlásai*, Repozitóriumok minősítése, 2012. Forrás: www.mtmt.hu/system/files/mtak_tamop_repozitoriumok_101_v4c.pdf (2015. 11. 15.)

34 MINERVA, könyvtári kisokos. Forrás: minerva.mtak.hu/?page_id=1058 (2015. 11. 15.)

35 BARTON-PÁL: *i. m.*, 3.

36 KOLTAY Tibor: *A tudomány és az új média viszonyáról*, Magyar Tudomány, 2014. március. Forrás: www.matud.iif.hu/2014/03/11.htm (2015. 11. 15.)

Andreas Kaplan és Michael Haenlein megfogalmazásában a közösségi média „internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom”.³⁷

A közösségi média alkalmazásait a különböző kiadók is beépítik szolgáltatásaikba annak érdekében, hogy szolgáltatásaik online jelenlétét megszilárdítsák.³⁸ A 2000-es évek elején megjelentek azok a közösségi oldalak, amelyeket a tudomány művelőinek szántak. Ilyen például:

- Az *Academia.edu*, amit Richard Price indított 2008 szeptemberében. Ez a közösségi média 2015 végére 29 millió regisztrált felhasználónak biztosít nyílt hozzáférést a tudományos dokumentumokhoz,³⁹
- A *ResearchGate.net* szabad hozzáférést garantál a keresés funkcióhoz a különböző szakfolyóiratok cikkei között, melyek egy több mint 30 millió bejegyzést, 8 millió felhasználót tartalmazó, és folyamatosan bővülő adatbázisban található. Az oldalt 2008-ban indította Ijad Madisch, Sören Hofmayer és Horst Fickenscher Németországban.
- A *LinkedIn.com* némileg hibridnek tekinthető, mivel nemcsak kutatók, hanem számos szakma művelői is használják. A 2003-ban elindított, 2011-ben az amerikai tőzsdére bevezetett céget Reid Hoffman vezeti. A több mint 332 milliós tagsággal a LinkedIn magasan a versenytársai előtt jár.

Nagy vihart kavart a felhasználók körében a 2013 elején napvilágot látott hír, mely szerint az Elsevier kiadóvállalat megvásárolta a *Mendeleyt*, a 2008 óta működő, eddig független hivatkozáskezelő és -megosztó, a kutatók körében közösségi oldalként is funkcionáló szolgáltatást. Bár az új tulajdonos rögtön igyekezett biztosítani a közel 2,3 millió felhasználót arról, hogy az ingyenesség és a színvonal továbbra is megmarad. A Mendeley ellentmondani látszik annak, amit az új média általános elvei sugallnának. Lehetővé teszi ugyanis, hogy a rendszer a kutatók oldaláról zárt maradjon, tehát számos funkció zártkörűvé tehető, vagy ki is zárható belőle a nyilvánosság.⁴⁰

Az OA folyóiratok célja, hogy a cikkeket minél szélesebb körben terjesszék, s azokhoz minél több kutató és érdeklődő hozzáférjen. Az elektronikusan publikált kutatási eredmények díjmentes rendelkezésre bocsátása a tudományos információt jobban láthatóvá és könnyebben elérhetővé teszi, azzal a pozitív eredménnyel, hogy gyorsabban hivatkoznak rájuk. Mindez megnöveli a folyóirat elismertségét. Az OA folyóiratok cikkei eredeti publikációk, a megjelenés előtt szakmai bírálaton esnek át.

Az Open Journal Systems (OJS) egy olyan folyóirat-menedzselő és publikáló rendszer, amelyet a kanadai Simon Fraser University Public Knowledge Project kormányzati támogatásból fejlesztett ki azért, hogy kiterjessze és gazdagítsa a kutatáshoz való hozzáférést.

37 Andreas M. KAPLAN, Michael HAENLEIN: *Users of the world, unite! The challenges and opportunities of Social Media*, Business Horizons, Vol. 53. Issue 1., January–February 2010, 59–68.

38 Ellen COLLINS: *Social Media and Scholarly Communications: The More They Change, the More they Stay the Same?* = szerk. Deborah SHORLEY – Michael JUBB: *The Future of Scholarly Communication*, Facet, London, 2013, 89–102.

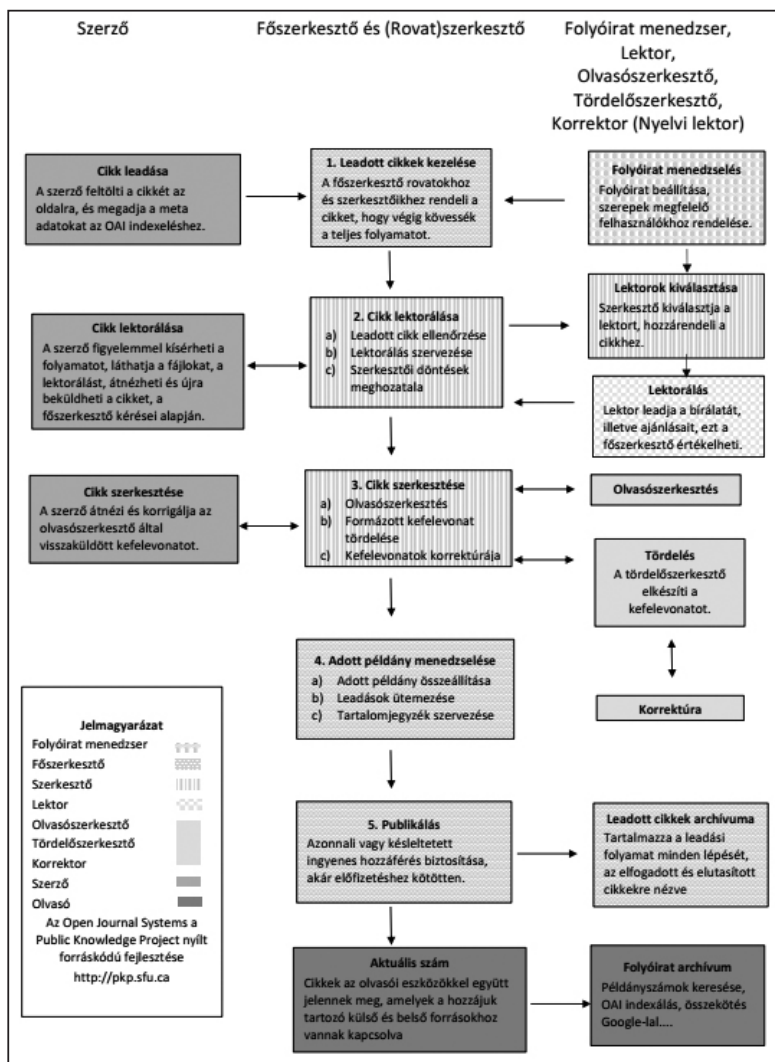
39 Richard PRICE: *The Future of Peer Review*, TechCrunch. Retrieved, 2012. Forrás: techcrunch.com/2012/02/05/the-future-of-peer-review/ (2015. 11. 15.)

40 COLLINS: *i. m.*, 1.

A rendszer figyelemmel kíséri a teljes szerkesztési folyamatot, a cikkek leadásától a megjelenésig és az indexelésig. A rendszer nyílt forráskódú és ingyenesen elérhető.⁴¹

Az 1. ábra mutatja be az OJS szerkesztési és publikálási folyamatát. A szerkesztőségi szerepek nem változnak, tehát nem a rendszergazda válik az újság főszerkesztőjévé, hanem a menedzselés helye és módja változik. Minden szerkesztési lépés az OJS-en belül történik, és a rendszer nemcsak tárolja a dokumentumokat, hanem naplózza is a tevékenységeket, valamint statisztikákat is készít.⁴²

1. ábra • Az OJS szerkesztési és publikálási folyamata (saját szerkesztés)



41 Open Journal Systems honlapja. Forrás: pkp.sfu.ca/ojs/ (2015. 11. 15.)

42 Open Journal Systems Stats. Forrás: pkp.sfu.ca/ojs/ojs-usage/ojs-stats/ (2015. 11. 15.)

A publikáló szemszögéből a változás csupán annyi, hogy a cikkeket, a javításokat nem e-mailen küldi el a szerkesztőségnek, hanem a rendszerbe tölti fel, és így juttatja el közleményét a megfelelő helyre. A főszerkesztő szerepe továbbra is a koordinálás, illetve a vezetői döntések meghozatala. A szervezés oroszlánrésze a rovatszerkesztőké, akikre a folyamatábrán „Szerkesztő”-ként hivatkozunk. Ők tartják a kapcsolatot a szerzőkkel, választják ki a lektorokat, illetve rendelik hozzá a cikkekhez, valamint tartják a kapcsolatot az olvasószervezőkkel, a tördelőszerkesztőkkel, a nyelvi lektorokkal (az ábrán „Korrektor” néven szerepelnek), hogy a publikálás előtt minden anyagot készen a főszerkesztő „kezébe adjon”. Végül a főszerkesztő összeállítja a folyóirat aktuális példányát, és publikálja a rendszeren keresztül.

Az OJS összeköthető az ismert adatbázisokkal, pl. a Google Scholarral, így a folyóirat cikkei gyorsan indexelhetőekké válnak. Fontos kiemelnünk, hogy a rendszer minden lépést adminisztrál, tehát pl. az el nem fogadott közlemények is a rendszerben maradnak, a szerkesztési folyamat szempontjából visszakereshető állapotban. A folyóirat-menedzser felel a rendszer és a szerkesztés folyamatában résztvevők zökkenőmentes „kommunikációjáért”.

4. TUDOMÁNYOS PUBLIKÁCIÓK KERESÉSE

1996-ban, a Google alapítóinak – Sergey Brin és Larry Page – az volt a céljuk, hogy működő digitális könyvtárakat hozzanak létre. Ötletük pedig a következő volt: a jövőben, amikor majd a könyvgyűjteményeket nagy mennyiségben fogják digitalizálni, az emberek egy „feltérképező robotot” fognak használni a könyvek indexelésére, és a közöttük lévő kapcsolatok elemzésére, bármely adott könyv relevanciáját és hasznosságát olyan módon határozva meg, hogy a más könyvekben lévő idézetek számát és minőségét követik figyelemmel.⁴³ A *Google Tudós* (eredetileg Google Scholar) a Google tudományos keresője, amely különféle témájú és formájú tudományos publikációk között keres. 2004. november 18-án indult, mára közel 160 millió dokumentumban, szinte minden online elérhető referált folyóiratban keres.⁴⁴

Az elérhetőség, kereshetőség lehetőségét a tudományos szakirodalom esetében üzleti alapon működő adatbázisok teremtik meg, jelenleg: a *Web of Science* (WoS) és a *Scopus*.⁴⁵

A WoS a világon a legismertebb és leggyakrabban használt hivatkozási, illetve bibliográfiai adatbázis. Interdiszciplináris, heti frissítéssel közreadott anyagai a tudomány egész területére kiterjednek, 50 ezer könyvet, 12 ezer folyóiratot és 160 ezer konferenciaközleményt tartalmaz. Tudományos szempontok szerint rendszerez, lehetővé teszi a tudományometriai méréseket és a szerzői hivatkozások feltárását.⁴⁶

43 BÓTA László: *Internetes keresőrendszerek működése*, 2011. Forrás: www.tankonyvtar.hu/hu/tartalom/tamop425/0005_34_internetes_keresorendszerek_scorm_06/631_a_googlekeresrobot_httrtrtnete.html

44 Enrique ORDUÑA-MALEA, Juan Manuel AYLLÓN, Alberto MARTÍN-MARTÍN, Emilio Delgado LÓPEZ-CÓZAR: *About the size of Google Scholar: playing the numbers*, Granada, EC3 Working Papers, 18, 23 July 2014. Forrás: arxiv.org/ftp/arxiv/papers/1407/1407.6239.pdf (2015. 11. 15.)

45 HOLL András: *Információáradat és hullámvaglás*, Magyar Tudomány, 2013/4, 473–479. Forrás: www.matud.iif.hu/MT201304.pdf (2015. 11. 15.)

46 Miriam Anna DRAKE: *Encyclopedia of Library and Information Science*, New York, N.Y.: Marcel Dekker, 2004.

A 2004 novemberében indított *Scopus* a lektorált szakirodalom legnagyobb absztrakt- és citátum-adatbázisa. A több mint 5 ezer nemzetközi kiadótól származó, több mint 20 ezer kiadvány mellett a *SciVerse Scopus* gyors, könnyű és átfogóan használható eszközt nyújt a kutatóknak, amely jól megfelel a kutatási igényeknek a természettudományok, a műszaki tudományok, az orvostudomány, a társadalomtudományok, és az utóbbi időben már a humán tudományok területein is.

Magyarországon a *Magyar Tudományos Művek Tára* (MTMT) gyűjti össze a tudományos publikációkat, és amellet, hogy statisztikai adatokat szolgáltat, portált is biztosít majd a hazai tudományos eredményekhez. Az egységes keresés lehetőségeit az MTMT teremti meg, és utat nyit a szabadon elérhető teljes szövegek felé – már amennyiben ilyen rendelkezésre áll – a kiadóknál vagy a repozitóriumokban.⁴⁷

A WoS vagy éppen a Scopus nem helyettesítheti az MTMT-t, mert a humán- és társadalomtudományokat, a magyar nyelven publikált cikkeket ezek nem reprezentálják.⁴⁸

Hasonló megoldásokkal találkozunk Hollandiában (NARCIS), Malajziában (MyCite), Szlovéniában (SICRIS), Horvátországban (CROSB), Norvégiában (CRISTIN) és a Cseh Köztársaságban (Research and Development Information System).⁴⁹

5. A PRO PUBLICO BONÓBAN PUBLIKÁLÓK EMPIRIKUS VIZSGÁLATA

„A közigazgatás egy igazgatási tevékenység, amelynek célja az állami feladatok megvalósítása.”

⁵⁰ 2013 szeptemberében indult el az első Közigazgatás-tudományi Doktori Iskola a Nemzeti Közszolgálati Egyetemen. A *Közigazgatás-tudomány* interdiszciplináris jellegének megfelelően a Doktori Iskola hat kutatási területen – Közjog és közigazgatás, Állam és társadalom, Közmenedzsment, Állam és ökonómia, Közigazgatás a nemzetközi és európai térben és Emberi erőforrás területeken – kezdte meg a működését.⁵¹

A 2012 októberében alapított *Pro Publico Bono – Magyar Közigazgatás* független lap célja az általános államtudományok, kiemelten a közigazgatás-tudomány és a jogtudomány, a közmenedzsment és a közpolitika fejlődését szolgáló lektorált kutatások és szakmai tapasztalatok közlése.⁵² Az újság 2015 decemberétől OJS rendszert használ.

2015. decemberéig online formában 9 szám érhető el (2013/1–4., 2014/1–4., 2015/1), amelyekben 140 kutató publikált 135 tudományos közleményt, nemzetközi kitekintést, szakmai

47 HOLL András: *Az Akadémiai Könyvtár repozitóriuma, a REAL bővítése, gyarapítása, fejlesztése*, TMT, 60(2013)/4.

48 HOLL: *i. m.*, 3.

49 MAKARA Gábor: *MTMT ÉS MTMT2*, 2015, 19. Forrás: www.mtmt.hu/system/files/mtmt_ppt_2020_kedvesza_hu-mg_0.pdf

50 KALTENBACH Jenő: *Általános közigazgatási ismeretek*, 2012. Forrás: uni-nke.hu/downloads/egyetem/vtki/altalanoskozisgmtk.pdf (2015. 12. 15.)

51 ORBÁN Anna: *Az e-közigazgatási kutatások trendje: Áttekintés a nemzetközi és hazai irodalmak alapján*, Doktoranduszok Országos Szövetsége, Tavasz szél: Absztraktkötet, 2015, 485.

52 *Alapító okirat*, Pro Publico Bono – Magyar Közigazgatás szakmai, tudományos folyóirat. Forrás: uni-nke.hu/uploads/media_items/ppbmk-alapito-okirat-2015.original.pdf (2015. 11. 15.)

fórumot vagy szemlét. Ebből 113 egyszerős, 14 kétszerős, 3 háromszerős, 1 négy-, hét- és tízszerős, 2 pedig ötszerős közlemény volt.

Az itt publikálók közel 70%-a (97 fő) az MTMT-ben tag, 43%-a (59 fő) törzstag, oktató vagy témakiíró valamelyik magyarországi doktori iskolában. Az 59 fő doktori iskolával fennálló kapcsolata az alábbi megoszlás szerinti:

- 34%-a NKE Közigazgatás-tudományi Doktori Iskola,
- 6%-a NKE Rendészettudományi Doktori Iskola,
- 6%-a NKE Hadtudományi Doktori Iskola,
- 4%-a SzTE Állam- és Jogtudományi Doktori Iskola,
- 4%-a NKE Katonai Műszaki Doktori Iskola,
- 4%-a PTE Gazdálkodástani Doktori Iskola,
- 4%-a KRE Állam- és Jogtudományi Doktori Iskola,
- és 38%-a egyéb – összesen 51 doktori iskola, habilitációs bizottság, egyetemi doktori tanács.

A Pro Publico Bono – Magyar Közigazgatás lap szerzőinek⁵³

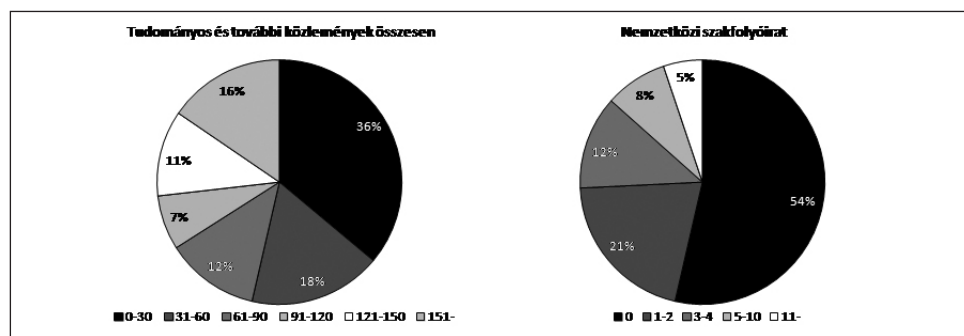
- 41%-a a Nemzeti Közszolgálati Egyetemen,
- 6%-a a Pécsi Tudományegyetemen,
- 4%-a az MTA valamelyik szervezeténél,
- 3%-a a Budapesti Corvinus Egyetemen,
- 16%-a másik egyetemen, főiskolán,
- 27%-a egyéb helyen dolgozik.

Azok a kutatók, akik regisztráltak az MTMT-ben, 5790 darab tudományos közleménnyel és 1931 további tudományos művel (összesen 7721 darab) rendelkeznek. Az MTMT szerint 262 nemzetközi szakfolyóiratban megjelent cikkel és 1350 megosztással rendelkeznek.

A vizsgált 97 szerző közül 35 fő 30-nál kevesebb, 17 fő 30–60 közötti, 12 fő 60–90 közötti, 7 fő 90–120 közötti, 11 fő 120–150 közötti, 15 fő pedig 150-nél több tudományos és további tudományos közleménnyel bír. (2. ábra)

A szerzők között volt olyan, akinek 500, és volt olyan, akinek 2 tudományos és egyéb közleménye volt rögzítve az MTMT-be.

2. ábra • Tudományos és további közlemények száma és a nemzetközi szakfolyóiratban megjelent cikkek száma az oktatók arányában az MTMT alapján (saját szerkesztés az MTMT alapján)



53 Forrás: www.mtmt.hu, www.doktori.hu és egyéb oldalak.

A publikálók között volt olyan, akinek nemzetközi szakfolyóiratban 52 darab cikke jelent meg, és van 52 fő, akinek egyetlenegy nemzetközi cikke sem volt. Nemzetközi viszonylatban 20 fő 1–2, 12 fő 3–4, 8 fő 5–10 és 5 fő 11-nél több megjelent szakcikkkel rendelkezik.

A nagy idézettségű adatbázisok – Web of Science, Scopus, Google Scholar, vagy Magyarországon az MTMT – mind számítják a Hirsch-indexet is a szerzői teljesítményeket összegző oldalukon. Meg kell azonban jegyezni, hogy az egyes adatbázisok egy szerzőnek csak az általuk szemlézett forrásokban megjelenő közleményeit veszik fel, így adatbázisonként más lehet a szerző Hirsch-indexe. Ebből a szempontból az MTMT annyiban előremutató, hogy egy-egy szerző teljes tudományos munkásságának feldolgozására törekszik. A tudóstårsadalom részéről már több bírálat érte a Google Scholar, mert a neten eddig a tudományos szakirodalomnak csak kisebb része jelent meg, így a kereső számos, papíralapú hagyományos szakirodalmat értelemszerűen nem figyel.

A közigazgatással foglalkozó kutatók h-indexeit kétféleképpen vizsgáltuk:

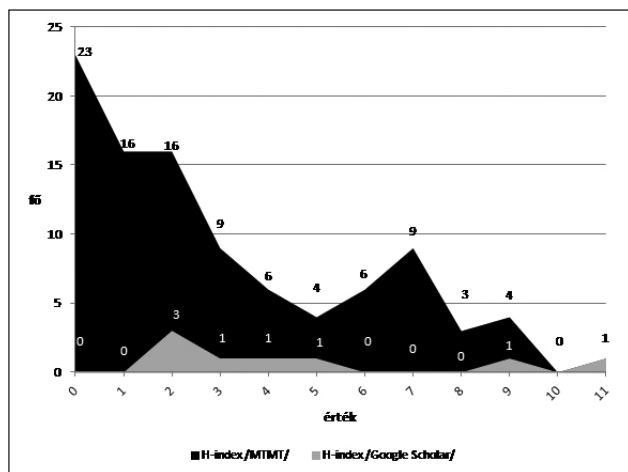
- MTMT által,
- és Google Scholar által mutatott értékeket.

Így az előzetes elvárásunk az, hogy az MTMT-ben szereplő h-index értékek minden esetben nagyobbak (esetleg egyenlőek) a Google Scholar h-indexével.

Az MTMT-ben megtalálható szerzők h-indexe 0 és 11 között változik, a Google Scholar esetén 8 személy regisztrált a rendszerbe.

Az MTMT szerint a vizsgált oktatók 24%-a 0-ás, 16%-a 1-es, 16%-a 2-es, 9%-a 3-as, 6%-a 4-es, 4%-a 5-ös, 6%-a 6-os, 9%-a 7-es, 3%-a 8-as, 4%-a 9-es és 1%-a 11-es h-indexszel rendelkezik. (3. ábra)

3. ábra • A h-index értéke és előfordulása közigazgatást kutatók körében az MTMT és a Google Scholar alapján (saját szerkesztés)



A statisztika alapján Hirsch szerint (a fizikában) 20 körüli értékkel húszéves szakmai múlttal az egyén sikeres kutató, 40-es index kiemelkedő kutatónak felel meg, míg 60-as index va-

lóban egyedülálló kvalitást jelez. Az egyetemi beosztásokat tekintve $h = 12$ körül lehet valaki docens, professzori kinevezéshez $h = 18$ körüli érték ajánlott. Az index erősen függ a szakterülettől, pl. a biológia és az orvostudomány területén a legjobbaknál a h értéke több mint kétszerese a fizikusokénak.⁵⁴

Magyarországon a legtöbb kutatási ágban a sok ezer hivatkozás és a 30 fölötti h -index nemzetközileg is kiemelkedő szakmai teljesítményre utal. Nehezebb egyértelműen eldönteni, kit tekintünk magyar kutatónak. Magyar származású, sőt a Magyar Tudományos Akadémia tagságát is elnyert világhírű kutatók tekintetében jogos lehet a büszkeségünk, de ők gyakorlatilag egyáltalán nem dolgoztak Magyarországon. Közéjük tartozik például több tízezer hivatkozással Barabási Albert László hálózatkutató (Google Scholar szerinti 111-es h -index), Somogyi Péter Pál és Buzsáki György idegkutató (MTMT szerint 94 és 51) vagy Gyulassy Miklós fizikus (80).

A nagyobb részben itthon működők közül az egyik legmagasabb mutatót egy fiatal, 36 éves fizikus, Csabai István mondhatja magáénak, ötvenezer fölötti idézettel és 83-as h -indexszel. Freund Tamás (85), az Akadémia alelnöke huszonhatezer idézettséggel és Vizi E. Szilveszter, az MTA volt elnöke (68) igen magas mérőszámok jelzik a hazai idegtudomány kiemelkedő teljesítményét.⁵⁵

A természettudományban viszonylag könnyebben lehet az idézettség alapján jellemezni a kutatói eredményességet, mint a társadalomtudományokban, de még a természettudományokon belül is igen különböző az egyes területeken elérhető eredmények számszerű értéke. Például a világhírű matematikus, az Akadémia elnöke, Lovász László (54) esete is mutatja, hogy a mérőszámok önmagukban nem abszolútizálhatók.

Az MTA Gazdaság- és Jogtudományok Osztálya MTA doktorai, tudomány doktorai, kandidátusai közül a legnagyobb h -indexe Lengyel Imrének (24) és Varga Attilának (23) a regionális gazdaságtan, Körösi Andrásnak (21) a politikatudomány, Kovács Imrének (19), a szociológia és Vastag Gyulának (19 – Google Scholar alapján), a tevékenységirányítás, ellátási hálókat kutatójának van.

6. A PRO PUBLICO BONÓBAN PUBLIKÁLÓK TUDOMÁNYOS LÁTHATÓSÁGÁT SEGÍTŐ ESZKÖZÖK HASZNÁLATÁNAK EMPIRIKUS VIZSGÁLATA

A tudományos folyóiratokban közölt cikkek elérésének költségei jelentős mértékben akadályozzák a kutatást. Az internet lehetővé tette a tudományos információk olcsó megosztását – az 1990-es évek elején a Los Alamos Nemzeti Laboratóriumban állították fel a jelenleg arXiv.org néven ismert, a Cornell Egyetem Könyvtára által üzemeltetett elektronikus különnyomat-lerakatot. Ebből nőtt ki a Nyílt Archívumok Kezdeményezés (*Open Archives Initiative = OAI*).⁵⁶

54 HIRSCH: *i. m.*, 1.

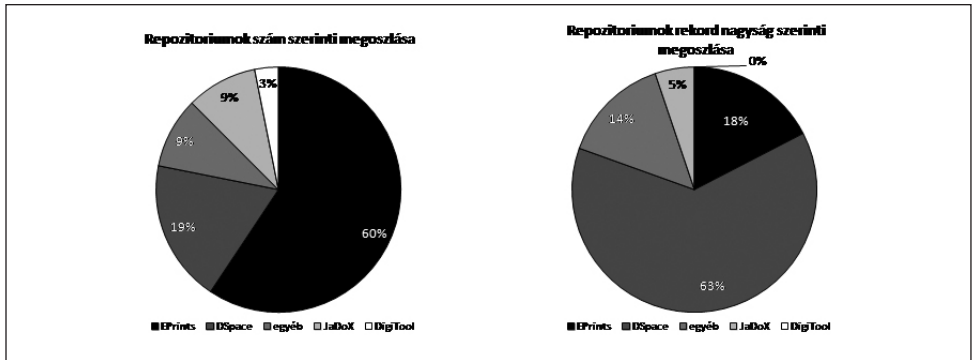
55 SARKADI Balázs: *Több tízezret érnek*, HVG, 2011. 12. 16. Forrás: mta.hu/sajtoszemle/tobb-tizezret-erne-129021/ (2015. 11. 15.)

56 Publikálás az interneten. Forrás: minerva.mtak.hu/?page_id=503#openacc (2015. 12. 15.)

Magyarországon jelenleg 32 repozitórium működik, és továbbiak felállítását lehet remélni. A repozitóriumnak nem kell feltétlenül az Open Archives Initiative keretében vagy nyoman fejlesztett repozitóriumszoftvert alkalmaznia, de meg kell jegyezzük, hogy számos ilyen szabad szoftver áll rendelkezésre (pl. EPrints, DSpace, JaDox stb.), melyek alkalmazása a repozitóriumokkal szemben támasztott technikai követelményeket (legfőképp az OAI meg-létét) vagy ezek megteremthetőségét, konfigurálhatóságát biztosítja.

19 (60%) egyetem és intézmény (pl. Budapesti Corvinus Egyetem, Közép-európai Egyetem, Szegedi Tudományegyetem és Magyar Tudományos Akadémia) EPrints, 6 (19%) egyetem és intézmény (Debreceni Egyetem, Eötvös Loránd Tudományegyetem, Kaposvári Egyetem, Nemzeti Közszerületi Egyetem, Semmelweis Egyetem és Magyar Tudományos Akadémia) DSpace, 3 (9%) egyetem (Miskolci Egyetem, Szent István Egyetem, Széchenyi István Egyetem) JaDoX repozitóriumszoftvert használ. (4. ábra)

4. ábra • Repozitóriumok szám és rekord szerinti megoszlása repozitóriumszoftver-használat alapján Magyarországon (saját szerkesztés)



Ezek a repozitóriumok közel 320 ezer folyóiratcikket, könyvet, könyvfejezetet és egyéb publikációkat tartalmaznak. 200 ezer (63%) rekordot DSpace, 55 ezret (18%) EPrints, közel 17 ezret (14%) JaDoX repozitóriumszoftverrel érhetünk el.

A *The Ranking Web of World repositories* független szervezet minősítése – mely figyelembe veszi a méretet, a Google Scholar szerinti láthatóságot – alapján a magyarországi rangsor (zárójelben a világranglistán elfoglalt hely):⁵⁷

- a Debreceni Egyetem (Debreceni Egyetem Elektronikus Archívuma) (272.),
- a Magyar Tudományos Akadémia (REAL – az MTA könyvtárának Repozitória) (313.),
- a Budapesti Corvinus Egyetem (BCE Doktori disszertációk archívum) (753.),
- a Szegedi Tudományegyetem (SZTE Doktori Értekezések Repozitória) (822.),
- ...

57 *The Ranking Web of World repositories: Hungary*. Forrás: repositories.webometrics.info/en/Europe/Hungary%20 (2015. 11. 15.)

– a Nemzeti Közszerzői Egyetem (Ludovika Digitális Tudástár és Archívum, LUDITA) (1679.).

A Pro Publico Bono – Magyar Közigazgatás lap szerzőinek lehetőségük van külső azonosítók használatára. Az azonosítók használatának több célja, haszna van:

- A mű elérése, olvasása: azonosítóval és hivatkozással egy kattintással el lehet érni a közlemény teljes szövegét.
- Ellenőrzés: azonosítókkal el lehet érni a közlemény adatait külső, indexelő adatbázisokban, katalógusokban, ami segít a közlemény metaadatainak ellenőrzésében, érvényesítésében.
- Értékelés: a külső adatbázisban történő indexelés a mű értékelésénél is felhasználható.
- Duplumkeresés: bizonyos azonosítók felhasználhatók a duplumok azonosítására.

Az MTMT-ben az azonosítókat csoportokban is lehet kezelni. A jelenleg használt csoportosítás:⁵⁸ (1) DOI, (2) Indexelő adatbázis, (3) Kiadói adatbázis, (4), Repoitóriumok, (5) Könyvtári katalógus, (6) Link, (7) Egyéb.

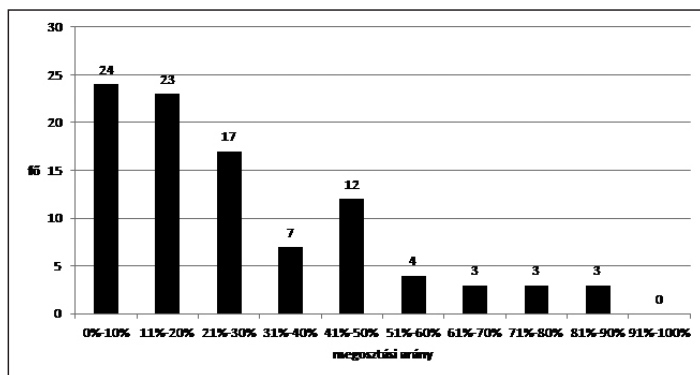
Olvashatóság/elérhetőségi beállítások (forrásközleményeknél):

- Gold: Kiadói honlapon vagy repoitóriumban szabadon olvasható
- Green: Repoitóriumban szabadon olvasható
- Restricted: Jogosultsággal olvasható
- Closed: Nem olvasható
- Embargo-r: Adott időpontig csak jogosultsággal olvasható
- Embargo-c: Meghatározott időpont után olvasható
- Pay: Díjfizetéssel olvasható

Az olvashatósági, illetve elérhetőségi beállításokkal elvileg minden tudományos és tudományos közlemény azonosítóval rendelkező műnek elérhetőnek kellene lennie!

Az MTMT-ben regisztrált 97 szerző közül 47 fő (0–20%) alig, illetve 9 fő (60%–) nagy arányban használ azonosítót. (5. ábra)

5. ábra • A Pro Publico Bono – Magyar Közigazgatás lap szerzőinek tudományos és további közleményei azonosítóhasználatának aránya az MTMT alapján (saját szerkesztés)



58 A külső azonosítók tulajdonságai és ajánlás kezelésükre. Forrás: www.mtmt.hu/system/files/kulso_azonositok_ajanlas.pdf (2015. 12. 15.)

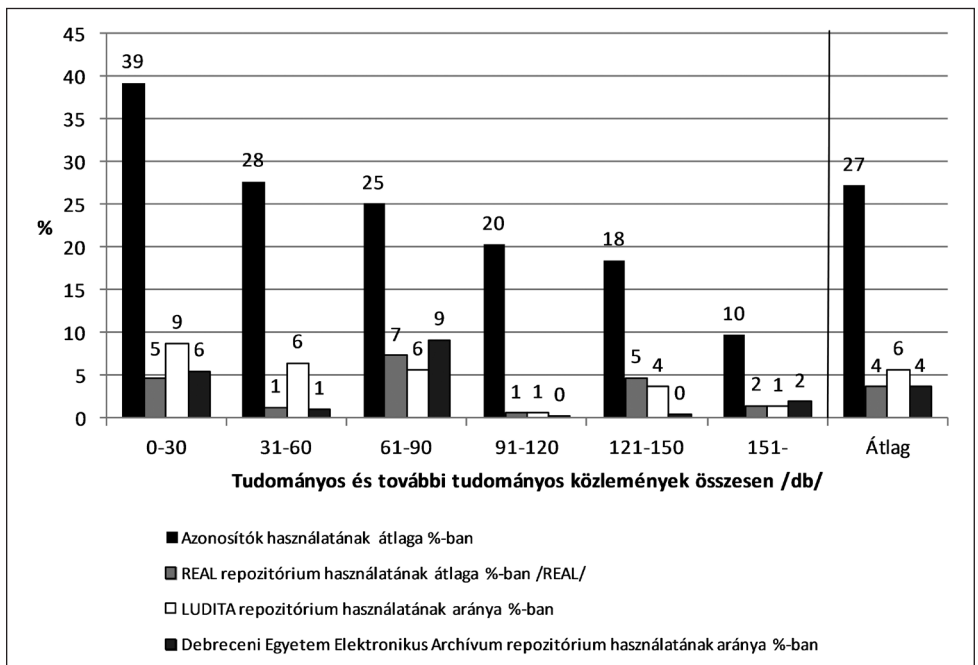
A repozitóriumi feltöltők munkáját könnyíti az MTMT-ből indítható repozitóriumi feltöltés lehetőségének megteremtése. A *SWORD protokollon* alapuló feltöltés az MTMT-ben 9 repozitóriummal (köztük a REAL-lal) valósítható meg. Az egyes repozitóriumok elérhetőségét a bejelentkezett kutató beállított munkahelye határozza meg (a REAL minden esetben elérhető).⁵⁹

Ha a repozitórium nem bír *SWORD protokollon* alapuló feltöltéssel, akkor azt *manuálisan* kell elvégeznie a szerzőnek vagy az adminisztrátornak, majd a feltöltés után kapott elérhetőséget (URL-t) azonosítóként kell rögzíteni az MTMT-be (ilyen pl. a LUDITA, Debreceni Egyetem Elektronikus Archívuma).

Empirikus kutatás alapján megállapíthatjuk, hogy

- a kevés tudományos és további publikációval rendelkezők nagyobb arányban (39%) használnak azonosítót,
- a mindenki számára elérhető REAL-t a szerzők alig 4%-a használja,
- a LUDITA-ban 60 vagy annál kevesebb tudományos vagy további közleménnyel rendelkező szerzőknél magasabb a használata, mint a REAL repozitóriumé,
- a Debreceni Egyetem Elektronikus Archívumának használata 30-nál kevesebb vagy 150-nél nagyobb közleménnyel rendelkezőknél magasabb, mint a REAL repozitórium használata. (6. ábra)

6. ábra • Tudományos láthatóságot segítő eszközök használatának az aránya a közigazgatást kutatók körében (saját szerkesztés)



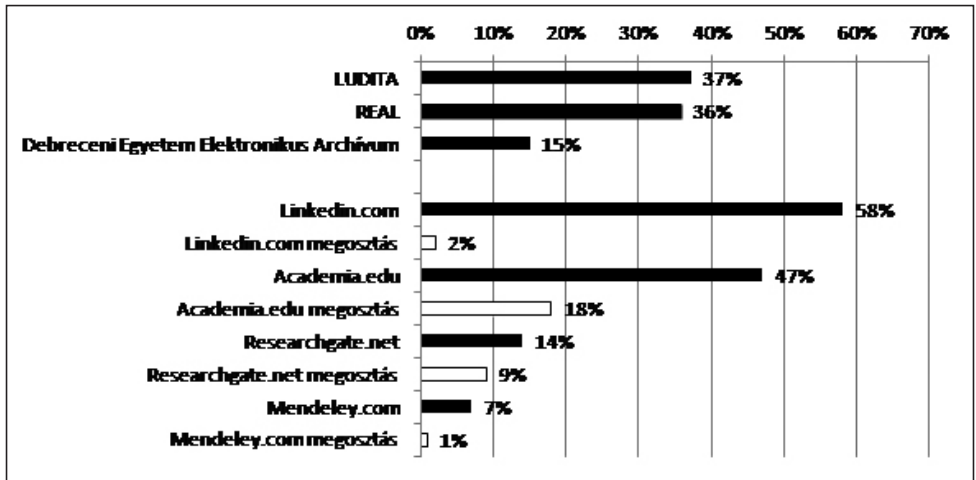
59 HOLL: i. m., 2.

1. táblázat • Az adott közösségi médiák és repozitóriumot működtető magyar egyetemek web-címei forgalmi adatainak globális sorrendje 2015-ben

Sorszám	Név	Globális sorrend
Közösségi média:		
1.	LinkedIn.com	14.
2.	ResearchGate.net	672.
3.	Academia.edu	727.
4.	Mendeley.com	17 673.
Magyar egyetemek és a Magyar Tudományos Akadémia		
1.	Magyar Tudományos Akadémia, Sztaki	24 309.
2.	Eötvös Loránd Tudományegyetem	37 061.
3.	Országos Széchényi Könyvtár	50 408.
4.	Szegedi Tudományegyetem	59 435.
5.	Debreceni Egyetem	62 215.
6.	Közép-európai Egyetem/Central European University	84 682.
7.	Budapesti Corvinus Egyetem	87 610.
8.	Óbuda Egyetem	92 352.
9.	Magyar Tudományos Akadémia	122 547.
10.	Szent István Egyetem	134 598.
11.	Miskolci Egyetem	144 789.
12.	Semmelweis Egyetem	152 947.
13.	Széchenyi István Egyetem	187 712.
14.	Nemzeti Közsolgálati Egyetem	319 234.
15.	Nyugat-magyarországi Egyetem	402 785.
16.	Kaposvári Egyetem	1 571 115.

A Pro Publico Bono 140 szerzőjéről elmondható, hogy 52 főnek a LUDITÁ-ban, 50 főnek a REAL-ben, 21 főnek a Debreceni Egyetem Elektronikus Archívumában található meg legalább egy közleménye.

7. ábra • Három repozitóriumban minimum egy közlemény, valamint a közösségi médiákba regisztráltak és a megosztások aránya a közigazgatással foglalkozók körében (saját szerkesztés)



A közösségi média alkalmazásáról megállapítható, hogy a legnépszerűbb regisztráció szempontjából a *LinkedIn.com* volt. Itt a felhasználók száma 81 fő (58%) volt. Majd az *Academia.edu* 66 fővel (47%), a *Researchgate.net* 20 fővel (14%), végül *Mendeley.com* 10 fővel (7%) következik. Tudományos és további közlemény megosztása az *Academia.edu*-n 25 főnél (18%), a *Researchgate.net*-en 13 főnél (13%) volt megtalálható.

A közösségi médiák használata azért is fontos tudományos és további közlemények megosztása szempontjából, mert jóval nagyobb látogatói számmal bír. (1. táblázat)

7. KONKLÚZIÓ

A tudományos teljesítmény értékelése, a tudományos kutatók minősítése során ma már egyre kevésbé veszik figyelembe az önálló tudományos szakkönyvek, monográfiák és tudományos igényű egyetemi tankönyvek szerzőségét. A minősítés mindinkább az ún. „hatástényező” alapján „rangosnak” tekintett folyóiratokban publikált cikkek és az ott megjelent hivatkozások száma alapján történik. A tudományos eredmény társadalmi, illetve oktatási hatása, széles értelemben vett „impakt”-ja így jobbára figyelmen kívül marad.

Számos lehetőség van egy kutató láthatóságának megjelenítésére, növelésére. Ezek mostanra leginkább az internethez kötődnek. A legnagyobbakat mások figyelik, így például a WoS és a Scopus. Azonban mi kutatók is tehetünk jobb megjelenésünkért, ennek egyik egyszerű formája a Google Scholar. Profil létrehozása után a Google Tudósban végzett keresés rögtön a kutatói profilt adja ki, számos fontos szcientometriai információval. Persze ehhez a

közleménynek *elektronikus formában* megtalálhatónak kell lennie. Ez lehet a *kiadónál*, a *tudományos közösségi médiáknál* vagy a *repozitóriumoknál*. A *kiadói* változatról az újság menedzsmentje gondoskodik az OJS használatával. A *közösségi médiába* való regisztrálás, feltöltés, valamint a *repozitórium* használata a publikáló, a szerző feladata.

Az empirikus kutatásaink során Google Scholar-regisztrációt alig találtunk. A közigazgatásban tevékenykedő kutatók tudományos láthatóságát javító eszközök használata a közösségi médiák és a repozitóriumok esetében hiányos (néhol alig mérhető), az MTMT-ben használt azonosítók tekintetében megfelelőnek tekinthető.

Az *Open Access* mellett számos érv létezik. Szakterülettől függően, bizonyos nyílt hozzáférésű publikációk akár háromszor magasabb hivatkozási szintet is elérhetnek, ráadásul a megjelenést követő rövidebb időn belül is hivatkoznak rájuk.⁶⁰ Az OA a bonyolult, komplex kutatási kérdések, problémák közös megoldásának ideális keretét adja. A nemzeti nyelven íródott tudományos publikációk továbbra is vezető szerepet töltenek be a bölcsészet- és társadalomtudomány terén. Ellenben, ha egy idegen nyelvű szöveg online is elérhető, növekszik az esélye annak, hogy észreveszik, akkor is, ha nincsen angol nyelvű absztraktja. A keresőmotorok, mint pl. a Google Scholar, a teljes szöveget indexelik, és a dokumentumok közötti kapcsolatot láthatóvá teszik.⁶¹ Az OJS használata természetesen semmiképpen sem jelenti a szerkesztői munka végét, hanem inkább annak egységes megvalósítását szolgálja. Mivel a rendszer végigköveti a szerkesztői munka összes lépését, ezért minden egyes cikk útja követhetővé válik, a beadástól a publikálásig. Minden szükséges információ kéznél lesz. Véleményünk szerint ez a munka hatékonyságát is növelni fogja.



SUMMARY IN ENGLISH: In the current article, the authors describe the concept of scientometrics, the types of measuring scientific achievement, the tools ensuring scientific visibility and some major search applications used for finding academic publications. A deeper insight is given into the quantity, quality and effect of the publications by researchers dealing with the field of the Hungarian public administration. The use of modern social media designed for researchers, the Open Journal System and the repository system is also presented in detail, which can have a contribution to enhancing the scientific visibility of scholars and researchers.

60 Stevan HARNAD, Tim BRODY: *Comparing the Impact of Open Access (OA) vs. Non-OA Articles in the Same Journals* = D-Lib Magazine, Vol. 10. No. 6., 2004.

61 Érvek az Open Access mellett. Forrás: www.open-access.hu/ervek (2015. 11. 15.)

Dr. Sasvári Péter (petersasvariphd@gmail.com) egyetemi docens elsőként gépészmérnöki, majd okleveles közgazdász diplomát, azt követően a társadalomtudományok, gazdálkodás- és szervezéstudományok területén PhD-fokozatot szerzett. A doktori dolgozatának címe „Az információs és kommunikációs technológia fejlettségének empirikus vizsgálata” volt, amit „summa cum laude” minősítéssel 2009-ben védett meg.

Fő kutatási területe a közsféra és a vállalkozások információsrendszer-használatának vizsgálata. Primer kutatást végzett külföldi egyetemeken bevonásával a kis- és középvállalkozások körében Ausztriában, Bosznia-Hercegovinában, Csehországban, Horvátországban, Lengyelországban, Magyarországon, Németországban, Olaszországban, Spanyolországban és Szlovákiában.

Az elmúlt évek tudományos munkásságáról elmondható, hogy több mint 75 közleményből 19 nemzetközi folyóiratban jelent meg, idézettségeinek száma meghaladja az ötvenet, 5 nemzetközi könyv szerzője volt. 2013. október 1. óta dolgozik a Nemzeti Közszolgálati Egyetemen. Sasvári Péter az NKE oktatási tevékenységébe is bekapcsolódott. A „Tudománymetria és publikációs stratégia – fókuszban az infokommunikációs stratégiák” doktori tárgy oktatásában és a tananyag fejlesztésében aktívan is részt vett.

Törley Gábor (Törley.Gabor@uni-nke.hu) adjunktus az Eötvös Loránd Tudományegyetem Informatikai Karán szerzett informatikatanári diplomát 2005-ben, és ebben az évben nyert felvételt a Kari Doktori Iskolába. A 2007–2008-as tanév őszi szemeszterében Erasmus-ösztöndíjat nyert el, és Helsinkiben végzett kutatómunkát, amelyvel doktori kutatásának alapjait rakta le. Doktori dolgozatának címe „Vizualizáció a programozástanításban” volt, amit „cum laude” minősítéssel 2014-ben védett meg.

Fő kutatási területe az oktatási módszerek fejlesztése, értékelése, különös tekintettel az e-learning használatának, a programozás- és biztonság tudatosság oktatásának fejlesztésére. Utóbbi témában átfogó kutatást végez a jövő közigazgatása humánerőforrásainak felkészültségéről, szükségleteiről.

Az elmúlt évek tudományos munkásságáról elmondható, hogy 19 közleményből 1 nemzetközi folyóiratban jelent meg, két egyetemi jegyzet szerzője vagy társszerzője volt. 2008. szeptember 1-je óta dolgozik a Nemzeti Közszolgálati Egyetemen, illetve jogelődjénél. 2014-ben a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Karának Kari Tanácsa megválasztotta őt a 2013–2014. tanév kiváló oktatójának.

nemzetközi kitekintés•

Lilla Mária JUHÁSZ – Csilla PAKSI-PETRÓ – Pedro REIS

VIRTUAL LEARNING ALL OVER THE WORLD GOOD PRACTICE FROM PORTUGAL

The world has changed with the development of electronic systems and educational systems also use the products of the virtual world. E-learning enables teachers to efficiently cooperate with students in different scientific issues; it connects people all over the world and helps the fast, flexible and efficient implementation of the new scientific and educational materials. The National University of Public Service (NUPS) established its E-Learning Centre in 2013, which became a modern education centre for innovative public service. To further develop and internationalize the system, it is beneficial to find good practices from other higher education institutions. In this paper we shortly introduce the e-learning system of the NUPS and the e-learning system of University Fernando Pessoa (UFP) (Oporto, Portugal) called Virtual University. We exchange views and experiences by sharing our practices in the hope of implementing common development projects in the future.

KEYWORDS:

training for civil servants, e-learning courses, Pro Bono, UFP-UV, virtual room, webinar, Sakai Program

• • • • • • • • • •

1. INTRODUCTION

For many years in Hungary the constant further-training of practicing public administration officials was not ensured centrally, it happened in an isolated way. However, the efficiency of public administration has become more important than ever. That is why in 2012 the Hungarian Government appointed the National University of Public Service (NUPS) as the institution responsible for the continuous training and retraining of the whole public administration staff. NUPS, as a centre of excellence, keeps developing special training programs and provides further training for thousands of public servants each year. NUPS,

nemzetközi kitekintés •

with the help of e-learning, provides high quality and effective training for civil servants at an affordable cost.

To develop and internationalize the Hungarian system, it is indispensable and highly beneficial to find good practices from other higher education institutions of the world. In this study, after shortly introducing the NUPS's e-learning system, we familiarize the readers with the e-learning system of University Fernando Pessoa (UFP) (Oporto, Portugal), called Virtual University.

2. E-LEARNING DEVELOPMENT AT NATIONAL UNIVERSITY OF PUBLIC SERVICE IN HUNGARY

The world has changed with the development of electronic systems and educational institutions make use of the products of the virtual world. At a time when change is faster than ever, a key advantage of e-learning is that it has quicker delivery cycle times than traditional classroom-based instructions.¹ E-learning is the new way to teach and to efficiently cooperate with students in different scientific issues. It can connect people all over the world and help the fast, flexible and efficient implementation of the new scientific and educational materials. In fact, research indicates that e-learning reduces learning time by at least 25 to 60 percent when compared to traditional learning.²

Analysing the Hungary situation, we can ascertain that this teaching method has become widespread in higher education. This innovation means that the modernization of higher education reflects the constant development of the world. E-learning has countless advantages compared to face-to-face learning methods. It can get to an unlimited number of users; that is why it is suitable for training numerous people. Advancement and efficiency are more important today for public administration than ever. Hence, the Hungarian Government decided to introduce e-learning to ensure further training of civil servants to save money, time, and energy.

In Hungary, especially in the public service, e-learning is a relatively recent phenomenon; however, the foundations have been laid down and its continuous improvement is under way. The National University of Public Service (NUPS) established its E-Learning Centre in 2013 and became a modern education centre for innovative public service. Unique and special training material is developed based on the needs of government staff. The university is using this teaching method for the training of practicing civil servants and sometimes for BA, MA courses; which means at least 100.000 civil servants and students per year participate in the e-learning programme. This is an easy and comfortable way for practising officials to improve their skills and knowledge online. The extensive circle of users requires modern e-learning solutions to suit their needs. Since practising public officials have

1 www.kineo.com/us/resources/new-to-elearning/the-benefits-of-elearning (13/12/15)

2 Brandon HALL: *Learning management and Knowledge Management. Is the holy grail of integration close at hand?*, 2001, www.brandonhall.com (13/12/15) and www.kineo.com/us/resources/new-to-elearning/the-benefits-of-elearning (13/12/15)

limited time beside their day to day work, the program owner has to elaborate time-saving solutions. The pedagogical objective of the e-learning method is to educate learners in the most effective and learner-centred way with clear understanding of the various topics and with the help of clear and user-friendly presentation of the teaching material, self-evaluation tests, providing additional features in order to intensify the learning experience.

The organisation establishing the Centre was the Institute of the Executive Training and Continuing Education (ETCE) responsible for organising the training, education and exams of all civil servants in Hungary, using the latest technology and training methodology: e-learning and blended learning. The main tasks of the ETCE are: to support career advancement in public service, to provide exclusive advanced training and examination system for Hungarian public administration, to do special trainings for public service, to re-train senior (retired) military and police officers to public administration and to operate new training systems for municipalities. In 2015 the growing demand for improvement received a new organisational background with the foundation Apertus Nonprofit Firm supported by the NUPS. This firm ensures further improvement and hosts the IT background for the successful education in public service.

The electronic training system for civil servants is called Pro Bono (probono.uni-nke.hu/nyitolap), which is a unique platform for organising and completing programs, trainings (face-to-face), e-learning and blended learning. The homepage is available only in Hungarian at the moment, simply because only Hungarian native speakers use it currently.

The operation of Pro Bono is divided between the participants: first, the training officers who are the human resource leaders of over 1800 institutions. Secondly, the training organizers who are responsible for organizing courses and exams on behalf of the institutions in charge (NUPS and program owners), and last but not least, the third group is the participants of the trainings, i.e. the civil servants. Civil servants are instructed to use the platform and to plan their own training programs on their own private page.

Currently there are more than 1800 training programs at Pro Bono.³ The great majority of these programs are created and managed by the public service institutions. These are the “internal programs” which meet the necessity of partaking special expertise for the institutions. But there is a considerable amount of programs provided solely by NUPS; namely 227 public service training programs and 33 leader training programs. The number of these programs is growing steadily thanks to the cooperation between the institutions and NUPS and to the EU funds.

NUPS is committed to share Hungarian experiences on further training of public and civil servants. Therefore it offers short-cycle training programmes in various fields, serving government needs on a large scale.⁴ Some of the main topics are: legislation, decision-making process of the government, management of central public administration, functions and procedures of central governance, public finances, budgeting, supervisory systems in public sector, e-public services, economy and development policies, labour policies, social policies, EU policies, IT security, cyber defence, communication, PR, media, HR management, local

3 www.apertus.hu/szolgalatasaink (27/12/15)

4 en.uni-nke.hu/study/training-for-civil-servants (23/12/15)

governance, health care policies, etc.⁵ But there are many other important programs, covering any institutional demand.

The benefits of online learning are plentiful. In this study we do not provide a detailed description of Pro Bono's operation; we merely give some revealing and insightful information and data on the matter. Pro Bono e-learning gives users the opportunity to create a fun and engaging training course through videos, interactive slides, and even games (sometimes humorous animated videos). The courses lead to better results by helping users retain more of the information learned. The online training system reduces costs that would normally be associated with classroom training, including travel, learning materials, venue, and catering. With Pro Bono the users can participate in their online courses at any time from any location – including from home, during down time at work, or anywhere else they feel appropriate. E-learning materials are stored online, so civil servants can access important resources any time they encounter a question or difficult situation.

There is a help desk for participants where they can download their electronically signed certificates, file a complaint report and fill in satisfaction questionnaires. These latest two are really useful functions, since they help developers get information on the efficiency of the program plus the problem areas identified by the complaints get addressed in the further development of the system. Pro Bono served 1863 institutions and 70481 public servants in 2015.⁶ The system operates with the participation of 300 teachers and trainers; there are 500–1500 users per day on Pro Bono.

E-learning development is still a work in progress; the next step is the incorporation of NUPS BA, MA and PhD course videos. It needs personalization to suit the bigger variety of programs to personal competences, and it needs additional portal support. E-learning means no boundaries. Users are able to participate in online courses from anywhere with an internet connection. This eliminates a lot of energy spent coordinating where and when a course will take place. And most importantly users are able to get real-time feedback during an online training course. Additionally, because everything is connected online, organizers can also get up-to-date analysis on how courses are going, and track the progress of individual employees. That is why the main aim for the future is to create a face to face, interactive teaching methodology, to form and establish a system of virtual rooms. These rooms would serve as interactive forums or chat rooms to share knowledge, experience and scientific results online with the participation of people located anywhere in the country or the world.

3. GOOD PRACTICE FROM PORTUGAL, INTERVIEW WITH PROF. PEDRO REIS

To develop the system established in Hungary, we have to find good practices in other foreign higher education institutions. In September 2015 we had the opportunity to visit the University Fernando Pessoa (UFP) in Porto, Portugal. Our host professor Prof. Pedro Reis,

⁵ Academic Report, National University of Public Service, 2014, 83.

⁶ Datas of the National University of Public Service, ETCE, 2015.

associate professor, head of the e-Learning Department UFP-UV (Virtual University) shared his views and experiences on the topic. He shared with us their good practices in the form of an interview. At the end of the interview we highlight shared points for future development, which can substantiate the future scientific and research activities of the universities. These activities can form the basis for the universities' future cooperation.

3.1. What is UFP-UV? What was the reason for creating the e-learning system?

How did you do that? What are you working on currently?

University Fernando Pessoa is funded and managed by Fernando Pessoa Foundation, which is its legal representative. UFP was recognized as a public interest organization by the Portuguese State in 1996 and is organised in three faculties (Health Sciences, Human and Social Sciences, Science and Technology) and one School of autonomous Health Sciences unit (Ponte de Lima College). The University is committed to contribute to the shaping of a truly inclusive European Area of Higher Education. Being a foundational University, UFP has never been market oriented. We are a solid private higher education institution with a strong academic focus and a constant concern for quality maintenance and improvement in what concerns a highly qualified teaching staff, physical infrastructures and equipments and its teaching, research and extension projects.

After approximately 30 years of on-site courses, in 2012, the decision was made at UFP to also offer distance courses.

We offer undergraduate, master and PhD courses. These are mostly from the *Faculty of Human and Social Sciences, including undergraduate courses such as Communication Sciences, Business Sciences, Business Management and Accounting, Criminology, Political Science and International Relations, Psychology, Social Work, and master courses such as Creativity and Innovation; Humanitarian Action, Cooperation and Development; Clinical and Health Psychology; Legal Psychology, Teaching and Management of Education, and PhD in Information Sciences.*

There are also postgraduate courses (for instance, Facial Expression of Emotion) and training courses (for instance Business English – elementary and intermediate).

Moreover, there are also blended-learning courses from different academic fields; e.g. Health Sciences (Nursing) and Technology (Computer Sciences).

Since 2012 about 300 national and international students have attended e-learning courses at UFP, in Portuguese, English, or Spanish.

This initiative represents a major contribution to the internationalization of the university, which is, at the current stage, among the most important of our strategic goals.

The implementation of Distance Education courses at UFP implied the creation of a new department, called UFP-UV (Universidade Virtual, that is Virtual University); it is a small department where I am in charge as Pedagogical Coordinator, there are two other permanent full-time collaborators (one for user support and content management and another one for technical support and development), and also some occasional trainees providing specific services to about 300 students and 80 faculty members – so far involved in this project.

3.2. What is Sakai Program and why is it so reliable?

The e-learning courses at UFP-UV use a *Learning Management System (LMS)* called Sakai. Developed by educators for educators, Sakai is a digital learning/teaching and academic collaboration environment that we customised to meet our needs and image.

The Sakai community is comprised of individuals and institutions that share a common commitment to enhancing teaching, learning and research. This commitment is reflected in how community members come together to pool knowledge, define the needs of academic users, create and share software tools, and support the adoption of the Sakai project. Participation from more than 350 of the world's leading institutions lends creativity, stability and longevity to this effort.⁷

In 2009, the UFP-UV team won the award Sakai fellow of the year, for the contributions made to the community of users, particularly with the creation of a tool, Site Stats, to see statistics and create field activity reports.

3.3. How did you manage to prepare teachers and students for using your e-learning system? How do you maintain it?

At the beginning of the implementation process, the aim was to give it an operational face, in order to make this teaching and learning process, new at the university, as comprehensible as possible for everybody to get involved (faculty, students and also some administrative staff). We were well aware of how challenging it was to adopt an approach which would be able to cover a significant number of people, since people would be heterogeneous, at the level of IT skills, for example. Additionally, this proved to be true not only for students but also for teachers, who, belonging to different generations and having different scientific backgrounds, naturally have very heterogeneous levels of computer skills.

Great emphasis has been placed on support technologies, and pedagogical models have been inspired by international best practices, adapted to our reality and carefully transmitted and discussed with teachers. Thus, continuous training and especially permanent support were and still are crucial to the project. Training and support to teachers are provided mostly F2F⁸ at the university e-learning department and support to distance students is provided in various forms: e-mail, phone, Skype and also original tutorials produced at the department and sent by email or delivered on the LMS.

The training program for faculty members focuses on methodological, pedagogical and technological aspects. One of the biggest challenges, at first, was indeed the fact that teachers were not prepared for e-learning. This required very personalized training, in small groups, within the same scientific field to better realize and share the difficulties that e-learning could represent to each group. This is complemented by constant assistance from a help desk devoted exclusively to this function.

⁷ sakaiproject.org/node/43 (09/09/2015)

⁸ F2F is IT slang meaning "Face-To-Face".

In the implementation of our e-learning comprehensive methodology, we had to insist with faculty members that courses would take place exclusively on the Virtual Campus of the university, which is equipped with appropriate state of the art educational technologies suitable for this purpose. This guarantees that students have online courses; furthermore, it is a guarantee for both teachers and the university, since their work is documented, and it can be demonstrated for national and international educational authorities how our e-learning courses work and what results have been achieved.

Other ways of communicating with students, by email or Skype, for example, are not prohibited, of course, but those are not to be confused with the official teaching-learning process. The latter occurs exclusively on the Virtual Campus of the university, whereas other contacts by email or Skype have to be considered as informal communication, as the equivalent of a corridor or cafeteria contact in an on-site context. Thus, in addition to focusing on the specific training program applying new technological educational tools, the training of faculty members involved a kind of *evangelization* to help bring about a teaching paradigm change.

3.4. Can you introduce us the development of the “virtual room”?

Although the open source LMS forms the basis of the virtual campus, other open source educational technologies were added in an integrated approach. Thus, students do not have to leave the UFP-UV Campus to attend their courses. Here, they find all the resources used in the teaching-learning process: different tools of the LMS, especially for written asynchronous activities; the Virtual Room, for synchronous oral contacts; videos of the recorded lessons from their teachers; and the Learning Objects (LO), each having a main pedagogical goal, depending on the chosen theme of the distance courses (mentioned at the beginning).

The recorded lessons are produced with Educ@st, a video management system for recorded lessons of faculty, which can simultaneously capture the speaker and their PowerPoint or Prezi presentations. The equipment is installed in the TV studio of the university where specialised technicians and our content manager assist teachers in the production of videos, which typically last around 15 minutes, mostly focusing on theoretical issues. These videos are then uploaded to a central server, edited and published in the LMS (Sakai), so that there is a controlled access to students. Access can be done by streaming or by downloading to PCs and mobile devices for later use, since the final publication is available in three distinct formats (Flash, Quicktime, iPod), which allows students to access their courses anytime, anywhere.

The Virtual Room is called COLIBRI, a Web Collaborative Environment. With the COLIBRI service, users can have video conference sessions for multiple purposes (lessons, webinars - sometimes with invited lecturers from other universities, tutorial sessions, dissertation supervision, and meetings among students for group work). It includes features such as live quizzes, screen or file sharing and mobile device access. It is also cross browser compatible.

The Virtual Room is also integrated with LMS (Sakai). Students can attend lessons and webinars live or see them later, since they are all recorded. Therefore students with professional commitments, who cannot attend the live lessons or webinars, have the option to see them later and thus learn what was discussed. Those who participated can also review the

lessons as a study strategy. The synchronous sessions in the Virtual Room provide moments for clarification, reflection, discussion or synthesis of subject matters.

Some LO were produced using freeware authoring tools, such as eXe Learning, Course-Lab, and especially Xerte (a fully-featured e-learning development environment for creating web content, with enriched media and rich interactivity). With licensed software, more sophisticated LO could eventually be produced, but we had to consider both budget restraints and the long learning curve necessary to achieve proficiency in a new software which is hard to conciliate with the rapid development of e-learning. This led us to choose, for the moment, easy-to-use, yet relatively powerful, e-learning authoring tools which offer programming-free WYSIWYG environment for creating interactive e-learning content which can be published in our LMS. In spite of this effort, we recognize that the creation and development of LO is one of the fields where our activity could improve, as I will mention later.

3.5. Did you have any problems or difficulties during the improvement? How did you manage to handle them?

The implementation of e-learning on a comprehensive scale has been progressive and in the future we are trying to develop more courses in purely e-learning formats, i.e., including recorded lessons, learning objects (multimedia and interactive modules), and other formative self-study materials (such as online tests).

We are well aware that not all scientific areas and not all education levels adjust equally to the development of multimedia and interactive LO. Furthermore, not all teachers have the same ability to interact with Instructional Designers in order to convert their working materials to e-learning formats.

However, with the adoption of an e-learning platform to complement F2F classes in 2004, the good practices of some teachers began to be known and appreciated by the community; students started asking teachers not yet using the platform to provide e-learning materials, schedule activities, allow online assignment submission, etc. In this case the former good examples excited students and pushed other teachers to adopt those good practices. We hope for a similar outcome in the case of e-learning courses. If certain courses provide students with attractive teaching materials, it creates a certain level of expectation that students will want to experience in other courses as well.

So we plan to encourage the use of diversified learning materials to make the courses more appealing, taking into account the adequacy of those materials to the nature of subject matters and the learning outcomes of each level (1st, 2nd or 3rd cycle).

Another cornerstone in an e-learning system is the assessment scheme. We are well aware that the online assessment system is not infallible, but, is there any system that can be considered as such? However, our efforts are focused on looking for solutions that offer more guarantees to ensure the credibility of the courses, which we consider a key factor to uphold. At present, written exams are conducted online, via Virtual Room, using application sharing, with remote supervision of the teacher. The audio and video channels of both the student and the teacher must be open. Actually, the use of webcam by the student is mandato-

ry; otherwise the exam cannot take place. In order to further improve these guarantees, we consider introducing changes in the future, such as adding software that helps to ensure the identification of students in the written tests; or eventually establishing partnerships with foreign higher education institutions or protocols with official entities (embassies, consulates) where international students can go to take written tests and exams.

3.6. Are you planning future development strategy – cooperation and joint programs – to spread your e-learning system worldwide?

Generally speaking, tertiary education is engaged in a strong process of internationalisation: global markets of educational services are developing, for example. An increasing number of institutions in non-English speaking countries now offer courses in English to overcome their linguistic disadvantage in attracting foreign students.

Nowadays, internationalisation is definitely a key strategic goal at UFP, which is seen as a mechanism that can be used for profiling institutions, increasing the recruitment of students and for developing partnerships, strategic alliances and networks with foreign institutions, in addition to being a means of improving the quality of education and research.

This strategy includes, among other things, the development of e-learning study programs in foreign languages, namely English, the establishment of joint degrees offered in collaboration with foreign partners, the development of international research cooperation and the planned use of EU programs.

4. THE FUTURE: COOPERATION IN E-LEARNING DEVELOPMENT

After closely examining the e-learning systems of NUPS and UFP we can identify several common points and challenges in the situation of both universities. These common points can be the basis for joint future research activities and development cooperation.

Both universities created stable and high quality systems, which perfectly suit the requirements of modern e-learning. At the beginning of the implementation processes, the aim was to give the system an operational face, in order to make this teaching and learning process as comprehensible as possible to everybody involved (faculty, students/civil servants and also some administrative staff). The users and the teachers are heterogeneous; the level of their IT skills, for example. That is why support technologies, and pedagogical models should be carefully conveyed and discussed with teachers. The implementation of e-learning systems on a comprehensive scale has been progressive and in the future both universities are trying to develop more courses in pure e-learning formats, i.e., including recorded lessons, learning objects (multimedia and interactive modules), and other formative self-study materials (such as online tests).

Certainly, there are some differences between the two systems apart from the IT solutions. One of the main differences is in the scope of recipients. UFP has developed distance education mainly for students – many of them living abroad – whereas the NUPS provides e-learning programs for practicing Hungarian civil servants, basically in Hungarian.

UFP offers courses in Portuguese, English or Spanish. We can observe another difference in the number of users. At UFP about 300 national and international students are attending e-learning courses, while at NUPS the Pro Bono served more than 1863 public administration institutions and 70481 public servants in 2015. But these are just the numbers; the two universities are facing similar challenges in the future from many points of view.

Designing an interactive and fun course through the use of multimedia or the more recently developed methods of gamification enhances the engagement factor and the relative lifetime of the course material. Studies have shown that gamification *enhances learner engagement and improves retention*. Thanks to the dozens of sophisticated learning tools available today, it is simpler to introduce gamification into a learning program.⁹ We think that using more picturesque, gripping programs would make the learning process much more efficient.

UFP-UV has already introduced the virtual room, which, from our point of view, can even raise the number of graduates per year. With e-learning, it is possible to gain instant access to users and professors/trainers from all parts of the world. Besides enabling teams from various geographies to collaborate on problem-solving challenges in real-time, these tools also bring with them other advantages like instant connectivity to subject matter experts; regardless of where they are located.¹⁰ It would create a win-win situation for the Hungarian system (users and institutions) too. Another potential in the virtual room is that the lecturer has the ability to host a guest lecture without having to spend much money. It can be done virtually, with cameras. The added benefit comes in when we are able to replay the lecture and gain even more out of it. Students that missed out can view the recording, or students that attended can watch it again to further their understanding.¹¹

As we have already mentioned before, one of the common challenges is the teacher's ability to use this tool. Not all teachers have the same ability to interact online, or with the Instructional Designers, in order to convert their working materials to e-learning formats. The program managers should take care of preparing the teachers and should ensure a nonstop helpdesk.

The assessment scheme is also an important keystone. UFP-UV is making efforts to find solutions that offer more guarantees to ensure the credibility of the courses. It would be an important question for the Hungarian system as well, if the virtual room opens.

Another common point is the implementation of more courses fully completed for pure e-learning formats, i.e., including recorded lessons, learning objects (multimedia and interactive modules), and other formative self-study materials (such as online tests).

Nowadays, internationalisation is definitely a key strategic goal for both institutions. Our discussions opened a new opportunity for cooperation to improve the missing details together to make both e-learning systems more efficient. It could be beneficial to cooperate and carry out projects together on international level.

9 elearningindustry.com/science-benefits-gamification-elearning (22/12/15)

10 www.talentlms.com/elearning/benefits-and-drawbacks-of-online-learning (22/12/15)

11 www.talentlms.com/elearning/benefits-and-drawbacks-of-online-learning (20/01/2016)

In order to provide distance learning programs, we believe that institutions should comply with quality standards, such as:

- have a clearly defined and stated mission, goals, and objectives;
- have reasonably attainable and clearly stated educational objectives, and educationally sound and up-to-date curricula that are supported by quality instructional materials and appropriate technology;
- provide satisfactory educational services;
- offer adequate student support services;
- have demonstrated ample student success and satisfaction through an outcomes assessment plan;
- have qualified faculty and competent administrators and staff;
- have fair admission policies and adequate enrolment agreements;
- advertise its courses/programs truthfully;
- be financially able to deliver high quality educational services;
- have fair and equitable tuition and refund policies;
- have adequate facilities, equipment, supplies, and record protection;
- conduct continuous research and self-improvement studies.¹²

The development of on-line platforms facilitates the cooperation between higher-institutions and helps the improvement of our teaching methods by implementing the achievements of the digital world.

Both universities are highly student-centred. We look forward to future cooperation and to carrying out joint research projects in order to make our systems more efficient and accessible for students and public officials alike.

12 www.deac.org/UploadedDocuments/2015%20Handbook/1-Pages-1-28-2015.pdf p. 6. (20/01/2016)

Lilla Mária Juhász (Juhasz.Lilla@vtki.uni-nke.hu) is the vice-director for project development at the National University of Public Service, Institute of Executive Training and Continuing Education, Hungary. She is also a doctoral candidate; her research fields are the educational systems of public administration, the ethics and integrity policy of public officials. She is the president of honour at the Association of Hungarian PhD and DLA Students (DOSZ), Public Administration Department. During her academic studies, she established the Hungarian community of PhD students in public administration science. In 2011, she took part in the establishment of the National University of Public Service (NUPS), she was the advisor and coordinator of the ministerial commissioner. She was the leader of the Centre for Hungarian State Reform Operative Programs at NUPS and managed ten EU programs during the period of 2013–2015. In 2015, she established the operation of the Institution of the Science of the State at NUPS. Currently she is planning the new developments of the public sciences and the Hungarian education system for public officials in the framework of 2015–2020 EU Development Strategy.

Csilla Paksi-Petró (csilla.petro@vtki.uni-nke.hu) is an assistant professor at National University of Public Service, Faculty of Public Administration, Institute of Career and Human Resources. Her research area is the public service carrier management, including further training and leadership training. She has five years practice in education/training: leadership skills, organisational development, communication, motivation and performance management, carrier management, time management, self-knowledge, conflict resolution, stress management, team-building and labour law. She also has five years practice in HRM as a practicing public administration expert: recruitment, interviews, questionnaires, assessment centre, development centre, further training, allowance system, job analyses and evaluation systems, outplacement. She was the manager of many public administration development projects financed by the EU such as recruitment program for one-stop shop officials (2013); job analysis project in the public service (2012-2013); Integral Evaluation System in the public service (2012-2013); leadership recruitment project in the public administration (2014).

Prof. Pedro Reis (preis@ufp.edu.pt) is Associate Professor at the Faculty of Human and Social Sciences at Fernando Pessoa University (Porto, Portugal) and Head of the e-Learning Department UFP-UV (Virtual University). He is co-founder of Centro de Estudos sobre Texto Informático e Ciberliteratura (Centre for Computer-produced Texts and Cyberliterature Studies), and researcher of several financed projects. He is co-director of the journal Cibertextualidades (Edições UFP). He developed a Post-Doctoral Research Project on e-Learning with the cooperation of the Instructional Technology and Distance Education (ITDE), Nova Southeastern University (NSU) (Florida, USA). He is currently collaborating with the IAEA (UN, Vienna) as Consultant on e-learning and Educational Technologist. His main research

interests are Experimental Literature; Cyberculture and Cyberliterature; Digital Humanities; E-learning; Educational Technology; Instructional Design, and e-Content Development. He published several books and articles and he lectured in Portugal, Sweden, Ireland, USA, France, Brazil, Spain, Holland, Italy, Senegal, Germany, Ghana and Austria.

Kiss Attila – Beláz Annamária

SZABÁLYOZÁS ÉS EGYSÉGESÍTÉSI TÖREKVÉSEK AZ IKT ÉS A TÁVKÖZLÉS VILÁGÁBAN. BESZÁMOLÓ AZ ITU 2015 KONFERENCIA EREDMÉNYEIRŐL ÉS ANNAK HÁTTERÉRŐL

Számottevően növekszik az IKT-szektor gazdasági jelentősége, részesedése hazánk és Európa gazdasági teljesítményéből. Ezzel párhuzamosan nő a területet szabályozó szervezetek, a Nemzetközi Távközlési Egyesület (ITU), az Európai Unió, és Magyarország felelőssége is, hogy megteremtsék az innováció, a fejlett távközlés, a hatékony piaci és állami elektronikus szolgáltatások nyújtásához elengedhetetlen infrastruktúrát és szabályozási környezetet. Az ITU 2015-ben Budapesten tartotta éves konferenciáját, ahol elsődleges feladatával, az infokommunikációs szektor nemzetközi együttműködésének megteremtésével és a hagyományos megoldásokról a digitális társadalomra való átállás támogatásával foglalkoztak a tagországok szakértői és az IKT-piac szereplői.

KULCSSZAVAK:

távközlés; ITU; Telecom World Conference; infokommunikáció; IKT-szektor; szabvány

• • • • •

1. BEVEZETÉS

Fennállásának 150. évfordulóján, 2015 októberében a Nemzetközi Távközlési Egyesület (International Telecommunication Union, ITU) Budapesten rendezte meg legrangosabb eseményét, hazánk látta vendégül a Telecom World Konferenciát. A rendezvény súlyát – emellett a kongresszus témáját adó távközlési és IKT-szektor szabályozásának fontosságát – jól mutatja, hogy azt hazánk miniszterelnöke nyitotta meg a 129 országból érkezett több mint

4000 résztvevő előtt,¹ majd Áder János köztársasági elnök mondott beszédet a jubileumi kongresszus gálaestjén. Ezzel a 2012 őszi, a virtuális tér veszélyeit és szabályozási nehézségeit vizsgáló Cyberspace Budapest nemzetközi konferencia után egy újabb, az infokommunikációs szektor egészét érintő,² annak fejlődési irányait nagyban meghatározó nemzetközi rendezvényt sikerült Magyarországra hívni. Ez fontos üzenetet hordoz a hazai és nemzetközi IKT-szektorok, kutatóknak, startupoknak, kkv-k és nagyvállalatok képviselőinek is, hiszen Magyarország az ITU alapító tagjaként ismét megerősítette, hogy kiemelt területként kezeli és támogatja az infokommunikációs ipart. Ugyanakkor felhívta a figyelmet arra is, hogy hazánk kiemelt területként kezeli a közigazgatásban az innovációt; a fejlett IKT-eszközöknek és elektronikus szolgáltatásoknak jobban be kell épülniük hazánk közszolgáltatásaiba.

2. AZ IKT-SZEKTOR GAZDASÁGI JELENTŐSÉGE

Az infokommunikációs technológia speciális tulajdonságokkal rendelkező innováció, melyet három jellemzője tesz oly sikeressé: mindenre kiterjed (társadalmi beágyazottsága alapján és ágazati szempontból is); a fejlődéssel csökkenti a felhasználók költségeit; valamint gerjeszti az innovációt, tehát elősegíti új termékek, szolgáltatások és folyamatok fejlesztését, kutatását.³ Térhódítása megállíthatatlannak látszik, a hétköznapi és társadalmi, üzleti életünk részévé vált. Az IKT-hoz kapcsolódó eszközök kereskedelmének növekedésénél (évi 30%) is jelentősebb az IKT-szektorhoz kapcsolódó szolgáltatások bővülése, az OECD 2015-ben publikált jelentése szerint a szolgáltatások exportján belül (world exports of services) az IKT aránya 2001 és 2013 között majdnem megduplázódott.⁴ Az IKT-szektor bruttó hozzáadott értékét (GVA) vizsgálva szintén pozitív képet kapunk, az Európai Unióban az ágazat több mint 7,7 millió főt foglalkoztat, és évi 640 milliárd eurót állít elő (összes GVA 5,4 százaléka).⁵

A 2012-es McKinsey-tanulmány szerint hazánk nemzetközi összehasonlításban is jól teljesít a szektorban, a magyar internetgazdaság GDP-hez való hozzájárulása, főként az IKT-val összefüggő exporttevékenységeknek köszönhetően a bruttó hazai össztermék 6,8%-át adta.⁶ A GVA-hozzájárulást vizsgálva szintén meghatározó jelentőségű az ágazat. A Századvég és az IVSZ közös kutatása kiemeli: „a digitális gazdaság az elmúlt években közvetlenül és

1 A konferencia legfontosabb eredményeit, számait és részletes programját lásd: Experience the best of ITU Telecom World 2015, telecomworld.itu.int/2015-highlights/ (2016. 01. 04)

2 Tobias FEAKIN: *International cyber security: a divided road*. Forrás: www.aspistrategist.org.au/international-cyber-security-a-divided-road/ (2016. 01. 04)

3 András NEMESLAKI: *ICT driven public service innovation* = ICT driven public service innovation: comparative approach focusing on Hungary, ed. András NEMESLAKI, National University of Public Service, Budapest, 2014, 10.

4 3,4%-ról 5,8%-ra növekedett a vizsgált időszakban. Lásd bővebben OECD: *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, 2015, 38. Forrás: dx.doi.org/10.1787/9789264232440-en (2016. 01. 04.)

5 Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége: *Economic Footprint kutatás és a digitális gazdaság mérésének új módszertana*. Forrás: ivsz.hu/projektek/digitalis-gazdasag-merese-kutatas/ (2016. 01. 05.)

6 Összehasonlításképpen ez az internet gazdasági (Internet contribution) arányszám Németországban 3,2%, az Egyesült Királyságban pedig 5,4% volt a vizsgált időszakban. Olivia NOTTEBOHM et al.: *Online and upcoming: The Internet's impact on aspiring countries*, McKinsey&Company, 2012, 83. Forrás: www.mckinsey.com/~/media/mckinsey/dotcom/client_service/high%20tech/pdfs/internet_in_aspiring_nations_report_april_2012.ashx (2016. 01. 04.)

mentum, jogszabály tartalmaz azonban kitekintő, határokon átívelő életviszonyokat is szabályozó látásmódot, különösen igaz ez az IKT-szektorhoz kapcsolódó életviszonyokra.¹² Azonban már a 19. században igény jelentkezett a nemzetközi vagy globális együttműködésre a távközlés területén, így születtek meg az első nemzetközi szabványügyi szervezetek.

3.2. Az ITU létrejötte és jelentősége

Párizs, 1865. május 17. Húsz európai ország képviselője türelmetlenül várja, hogy aláírásukkal hivatalosan is megszülessen a Nemzetközi Távíró Egyezmény, mely dokumentum végre megoldást nyújt azokra a kihívásokra, melyeket egy amerikai festőművész, Samuel Morse innovációja hozott magával.

Morse az 1830-as években áthajózott Európába, hogy mélyebben megismerkedjen a kontinens festészetével. Feljegyzései szerint a hajóúton valaki az elektromágnesről tartott neki előadásokat, és ettől kezdve csak az foglalkoztatta, hogyan lehetne a segítségével nagy távolságra jeleket továbbítani. Felhagyott a festészetrel, és 1837-re el is készült a berendezése, valamint a morzejelekként ismert kódrendszer tervei. A szabadság elnyújtása után csupán 7 évvel el is indult az első üzemszerű távírvonal Washington és Baltimore között.¹³

A világ és a távközlés ezzel visszafordíthatatlanul megváltozott. Hálózatok épültek ki, távíróközpontok épültek, azonban hiányzott egy nemzetközileg egységes rendszer, vagy az infrastruktúra fejlesztését koordinálni képes szervezet. Ezt a problémát orvosolta a fent említett párizsi egyezmény, mely létrehozta a Nemzetközi Távíró Egyesületet (International Telegraph Union), 1932-től Nemzetközi Távközlési Egyesületet (International Telecommunication Union). A századfordulóra egyre terjedő rádióadók egymást zavaró sugárzásai, és a rádióhullámok határokat nem tisztelő, interferenciát okozó terjedése miatt a frekvenciák is szűkös erőforrássá váltak, melyre egységes szabályrendszert kellett kialakítani. Ez szükségessé tette a nemzetközi frekvenciagazdálkodás bevezetését, mely a versengő igények leghatékonyabb kielégítése és valamennyi ország egyenlő jogainak biztosítása érdekében csak az ENSZ keretében valósulhatott meg.¹⁴

Az ITU 1947 óta működik az ENSZ szakosított szabványosító szerveként, 193 tagállamában közel 700 ágazati és társult tagja van. Elsődleges feladata a nemzetközi együttműködés megteremtése az infokommunikációs szabványosításban a hálózatok problémamentes összekapcsolása érdekében, különösen a rádióspektrum és a műholdas pályapozíciók globális felosztása területén.¹⁵ Világértekezletein, kutató- és munkacsoportjain keresztül ajánlásokat és jelentéseket fogalmaz meg, melyek ugyan nem kötelezőek a tagállam-

12 OECD: *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, 2015, 36. Forrás: dx.doi.org/10.1787/9789264232440-en (2016. 01. 04.)

13 Kenneth SILVERMAN: *Lightning Man: The Accursed Life of Samuel F. B. Morse*, Da Capo Press, Cambridge, 2004.

14 BAJÓ József et al.: *Korlátos erőforrásokkal való gazdálkodás az elektronikus hírközlésben* = Hírközlés-szabályozás, hírközlés-igazgatás hazánkban és az Európai Unióban, szerk. LAPSÁNSZKY András, Complex Kiadó, Budapest, 2013, III/1. fejezet.

15 Nyílt nap az ITU Telecom World 2015 konferencián. Forrás: www.kormany.hu/hu/kulgaszdasagi-es-kulugyminiszterium/hirek/nyilt-nap-az-itu-telecom-world-2015-konferencian (2016. 01. 04.)

mokra nézve, de azok tudományosan megalapozott eredményeket és jó gyakorlatokat tartalmaznak, egységes módszertant és tervezési rendszert biztosítanak. Ahogy az ITU jelenlegi főtitkára, Houlin Zhao kiemelte, „A kezdetektől fogva az volt a fő célunk, hogy segítsünk összekapcsolni az embereket és a világ országait egy nemzetközileg elfogadott szabályrendszer szerint felépített globális infrastruktúra által.”¹⁶

Bár más nemzetközi szervezetek is működnek a területen, így az Európai Távközlési Szabványosítási Intézet, vagy az EU rádióspektrum-politikai szervezetei, az ITU jelentősége töretlen, és az évek során számos, a kommunikációt érintő innovációval találta szemben magát. Bell 1876-os telefonjától a napjainkban jelen lévő tárgyak és szolgáltatások internetéig (Internet of Things, Internet of Services) szükség van nemzetközi szabványok felállítására. A globalizálódó világ új beavatkozási területeket is teremtett az ITU számára. Már nem „csupán” szabályalkotási munkát végez a szervezet, hanem speciális programjai, cselekvési és akciótervei vannak (pl. Connect 2020 Agenda), melyek magukba foglalják a kiberbiztonság, a klímaváltozás, a digitális szakadék, a nyílt internet, az esélyegyenlőség, a fiatalok képzésének és a fejlődő országok felzárkóztatásának kérdéseit.

A genfi székhelyű ITU 1971 óta rendezi meg éves Telecom World Konferenciáját. A rendezvényen az IKT-szektor legjelentősebb piaci szereplői, kutatói, a tagországok képviselői és nemzetközi szervezetek küldöttei gyűlnek össze, hogy technológiai és szakpolitikai kérdéseket vitassanak meg. Fontos, hogy ez az éves barcelonai mobiltelefon-kiállítással vagy a Las Vegas-i Consumer Electronics Show-val szemben nemcsak egy iparági rendezvény, hanem valamennyi tagország magas szintű képviselőinek találkozója, ahol kiemelt nemzetközi stratégiai célokról születik döntés.

3.3. Az Európai Unió céljai és szabályozásának alapjai

Az 1980-as évek végére az Európai Unióban világossá vált, hogy a gazdasági, társadalmi kohézió alapvető feltétele a korlátozásoktól mentes távközlési szolgáltatások biztosítása, ki kell alakítani egy dinamikus és nyitott távközlési közös piacot. Ehhez azonban nem elegendő a nemzeti hálózatok műszaki értelemben vett kompatibilitásának biztosítása, melyet az ITU szabványosító tevékenysége kialakíthatna, hanem rendelkezésre kell hogy álljanak az egyes szolgáltatások is valamennyi EU-s előfizető számára.¹⁷ E célból született meg az egységes távközlés-politika, megindult az európai távközlési piac liberalizá-

16 IMRE Dávid: *ITU Telecom World 2015 – Connecting the people, the countries and helping accelerate ICT innovatoin to improve lives faster*, Perspective, 2(2015)/2, 14–17.

17 HELLER Krisztina: *Távközlési reformok*, *Közgazdasági Szemle*, 42(1995)/3, 301–319. Forrás: epa.oszk.hu/00000/00017/00003/0306.html (2016. 01. 04.)

ciója, majd fokozatosan előtérbe került az ex-post versenyjogi szabályozás és az európai szabványok bevezetése.¹⁸

Az első szabályozók megalkotása óta eltelt közel három évtized, azonban az EU-nak továbbra is kiemelt feladata, hogy az egységes belső piac megteremtése érdekében tagállami és uniós szinten is jobban összehangolja a távközlési piacot, mint egyetemes közszolgáltatást,¹⁹ eltörölje a tagállamok közötti „digitális megosztottságot”,²⁰ majd tágabban értelmezve kialakítsa a digitális egységes piacot.

Komoly kihívást jelent azonban az Unió rendkívül fragmentált távközlési piaca, melyen körülbelül 200 távközlési szolgáltató osztozik, szemben a Kínában vagy az Egyesült Államokban működő 4-5 nemzeti szintű szolgáltatóval.²¹ Ez a közös európai piacon elősegítheti a piaci verseny kialakulását, és a szolgáltatási díjak csökkenését is, de az egységes feltételek garantálása, valamint a magánszféra és az adatok biztonsága, a mobilitás és interoperabilitás megteremtése, a szolgáltatások árának közelítése komolyabb szabályozást igényel.

A telekommunikációs infrastruktúrához való hozzáférés néhány tagállamban továbbra is bonyolult és költséges, valamint a szolgáltatások igénybevételének díjai között országoként jelentős különbségeket tapasztalhatunk, igaz ugyanakkor, hogy a nem uniós európai országokhoz képest azok még mindig jelentősen kedvezőbb áron elérhetőek.²² Egy 2014-es bizottsági jelentés kiemeli azt is, hogy a mobil távközlési szolgáltatások díja magasabb az EU-ban, mint az Egyesült Államokban, de ott többet is használnak ezeket, ezáltal magasabb a felhasználónkénti átlagbevétel, mint az Unióban.²³

Az Európa 2020 stratégia hét pillérének egyike az információs és kommunikációs technológiákban rejlő lehetőségek hatékonyabb kiaknázását tűzte ki célként az innováció, a gazdasági növekedés és a haladás előmozdítása érdekében. E pillér, az Európai Digitális Menetrend 2010–2020 feladata az egységes digitális piac létrehozása, melynek

18 Az Európai Bizottság 1987-ben tette közzé a távközlési piacának kialakítását célzó stratégiai dokumentumát, a *távközlési szolgáltatások és berendezések közös piacának kialakításáról szóló Zöld könyvet*, melyet szisztematikusan jogalkotás követett a piacsabályozás és a fogyasztóvédelem területén. 1988–1996 között meghatározó szerepe volt a liberalizációs és harmonizációs irányelveknek, majd a 2000-es években (2002 – *New Regulation Framework*) a re-reguláció, azaz a hatásos verseny kialakulását és fenntarthatóságát ösztönző jogszabályi környezet kialakítása került a középpontba. TÓTH András: *Versenyjogi szabályozás és jogalkalmazás az elektronikus hírközlés vonatkozásában* = PhD tanulmányok 3., szerk. ÁDÁM Antal, Pécs, 2005, 390–392.

19 Lásd többek között az Európai Parlament és a Tanács 2002/22/EK irányelve (2002. március 7.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról (Egyetemes szolgáltatási irányelv)

20 A 2013-ban kiadott „*Behálózott kontinens*” távközlési piaci reformcsomag továbbra is kiemelt célként nevesíti a nyílt internet jogi védelmét és a hálózatsemlegességet, valamint az egységes hírközlési piac megvalósítását (pl. az EU 28 tagállamára érvényes működési engedély a szolgáltatóknak). A célokat rögzítő jogalkotási folyamat eredményeként 2015. november 25-én született meg az Európai Parlament és a Tanács (EU) 2015/2120. rendelete.

21 Kerstin GUNTER: *Opening Speech ITU Telecom World 2015*, 2015. 10. 12. Forrás: www.youtube.com/watch?v=IRW39sLdOBs (2016. 01. 04.)

22 European Commission: *Broadband Internet access cost (BIAC) 2014*. Forrás: ec.europa.eu/digital-agenda/en/news/study-retail-broadband-access-prices-2013-smart-20100038 (2016. 01. 04.)

23 European Commission: *Implementation of the EU regulatory framework for electronic communications – 2014* (Brussels, 14. 7. 2014 SWD(2014) 249 final). Forrás: ec.europa.eu/newsroom/dae/document.cfm?doc_id=6474 (2016. 01. 04.)

keretében az Európai Bizottság új szabályozási eszközökkel elő kívánja segíteni a hálózatfejlesztési befektetéseket,²⁴ amellett, hogy nagyobb választékot és több védelmet garantálna a távközlési szolgáltatások fogyasztóinak.²⁵ Az egységes piacot egységes hatóságok felügyelnék a jövőben, tovább szabványosítanák, és szélesebb kör számára elérhetővé tennék a legújabb távközlési infrastruktúrát is.²⁶ E fejlesztések lehetőségeket nyitnak meg a gazdaság e-kereskedelmen keresztül történő fellendítésére, megkönnyítik a vállalkozások számára a közigazgatási és pénzügyi előírásoknak való megfelelést, és az e-kormányzáson keresztül erősítik a fogyasztók jogait. A digitális egységes piacon belül kidolgozott piaci és kormányzási szolgáltatások az elektronikus és mobilplatformokon egyaránt fejlődhetnek, és egyre inkább jelen vannak mindenütt, bármikor, bárhol és bármely eszközön.²⁷

A Bizottság által 2015 májusában közzétett „Európai digitális egységes piaci stratégia” célzott intézkedéseket tartalmaz, melyeket 2016 végéig kell végrehajtani. Az intézkedések között külön fejezetben foglalkoznak a távközlési reformmal és a fejlett digitális hálózatok, valamint az innovatív szolgáltatások számára az egyenlő versenyfeltételek megteremtésével. Célja a nagy sebességű széles sávú infrastruktúrába való beruházások ösztönzése és a szabályozási intézményi keret továbbfejlesztése.

A közigazgatásban is egyre nagyobb az igény a gyorsabb és biztonságosabb ügyintézés iránt, az okostelefonokhoz és az intelligens online szolgáltatásokhoz szokott ügyfelek elvárásai mellett a hatékonyság növelése és az átlátható közigazgatási szolgáltatások érdekében is szükséges a telekommunikációs és széles sávú fejlesztések mielőbbi megkezdése, az e-közigazgatás előtérbe helyezése. A stratégia ezért ismerteti az EU e-kormányzati cselekvési tervét is, mely a bürokráciacsökkentés érdekében előírja az európai vállalkozói nyilvántartások összekötését, a nemzeti rendszerek átjárhatóságának biztosítását és az egyszerű adatközlés előmozdítását. A stratégia megvalósulása esetén a Bizottság a teljes mértékben működő digitális egységes piactól azt várja, hogy évente akár 415 milliárd euróval növelheti az EU gazdaságát.²⁸ A közelmúltban komoly előrelépés történt az európai nyílt internet (netsemlegesség) biztosítása és a roamingdíjak eltörlése érdekében is.

24 A stratégiával megszülető szabályozás a meglévő technológia kiterjesztése helyett az innovációra fókuszál, a fejlettebb megoldások átvételét részesíti előnyben az állami támogatások odaítélésének szabályozásán keresztül. Lásd KÁNTOR Zsófia, TORMA Gergely: *Költhetünk rá? Az állami támogatások megengedhetősége a széles sávú fejlesztések megvalósítása körében az Európai Unióban* = A verseny hálójában. Aktuális versenyjogi kérdések a hírközlés liberalizációja terén, szerk. VALLYON Emese – VITTAJ Melinda, ELTE Bibó István Szakkollégium a Felelős Értelmiségért Alapítvány, 2014, 66.

25 Az Európai Digitális Menetrend összefoglalója. Forrás: eur-lex.europa.eu/legal-content/HU/TXT/?uri=URISERV%3Aasi0016 (2016. 01. 04.)

26 BÁRÁNYNÉ Sülle Gabriella: *Egységes európai digitális piac 2015-re?* Média, kábel, műhold, 2013/9.

27 A mindenütt jelen levő digitális egységes piac. Forrás: www.europarl.europa.eu/atyourservice/hu/displayFtu.html?ftuId=FTU_5.9.4.html (2016. 01. 04.)

28 Európai Bizottság – Sajtóközlemény: *A Bizottság 16 kezdeményezése az európai digitális egységes piac létrehozására*. Forrás: europa.eu/rapid/press-release_IP-15-4919_hu.htm (2016. 01. 04.)

3.4. IKT és a közigazgatás viszonya Magyarországon

A professzionális, átlátható és biztonságosabb ügyintézés iránti igény egyre inkább ösztönzi az EU-tagállamokat, hogy az e-közigazgatás megvalósításához szükséges telekommunikációs és széles sávú fejlesztéseket előtérbe helyezték. A területen határokon átívelő fejlesztési stratégiával rendelkező országok, mint például Németország, a nemzetközi szervezetek bevonásával alakítja ki fejlesztési céljait, együttműködve az ITU, az Internet Governance Forum, vagy az OECD szakértőivel.²⁹

Hazánkban is kiemelt cél a közszolgálat IKT-korszerűsítése, 2007 és 2013 között jelentős mértékben növekedett a szektorba érkező állami támogatás. A Nemzeti Fejlesztési Ügynökség 2014-es kimutatása szerint a fejlesztések finanszírozása főként EU-s kohéziós és strukturális alapokból történt, ebben az időszakban 441 Mrd forint összegben kötöttek szerződéseket IKT-fejlesztésekre, ezek közül kiemelkednek az EKOP és az ÁROP fejlesztések, melyek a szűken vett e-kormányzat területére irányultak.³⁰

Már az 1960-as évektől jelen volt az informatika a közigazgatásban, de az ágazati szervezési és számítástechnikai intézetek többnyire adatfeldolgozó feladatokat láttak el. 1971–1990 között zajlott a számos alapnyilvántartást létrehozó (népesség-, ingatlan-, gépjármű-nyilvántartás stb.) Számítástechnikai Központi Fejlesztési Program, és utóda, az Elektronizációs Gazdaságfejlesztési Program. A rendszerváltást követő Magyar Információs Társadalom Stratégiának, és az annak részeként elkészült eKormányzat programnak napjainkig érezhető hatásai vannak. A MITS és az azt követő fejlesztési programok fogalmazták meg az elektronikus közigazgatással szemben támasztott követelményeket (pl. interoperabilitás, ügyfélközpontúság, hatékonyság), valamint kijelölték a fejlesztési területeket (pl. tudás, front- és back-office). Az e-közigazgatás megjelent a Digitális Megújulás Cselekvési Terv 2010–2014 stratégiában, és annak a Nemzeti Közigazgatási Kommunikációs Infrastruktúra programjában, valamint később a Magyar Programban is. A Nemzeti Infokommunikációs Stratégia (2014–2020) határozza meg hazánk aktuális digitális infrastruktúrára, a lakosság és a kvk-k digitális kompetenciáira, a digitális gazdaságra és a digitális államra vonatkozó fejlesztési programját. Pozitívum, hogy a stratégia pillérenkénti helyzetelemzése több helyen figyelembe veszi a korábban említett nemzetközi szervezetek statisztikai adatait, ezekre építve jelöli ki az elérendő célokat.

A digitális állam és digitális infrastruktúra pillérek célrendszeréhez illeszkedik a Közigazgatás- és Közszolgáltatás-Fejlesztési Operatív Program (KÖFOP), melyben 342 Mrd Ft jut a közigazgatás fejlesztésére, az állampolgárok számára nyújtott kormányzati szolgáltatások javítására.

29 OECD: *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, 2015, 36. Forrás: dx.doi.org/10.1787/9789264232440-en (2016. 01. 05.)

30 NEMESLAKI András: *E-közszolgáltatásfejlesztés*, Nemzeti Közigazgatási Egyetem Közigazgatás-tudományi Kar, Budapest, 2014, 17.

3.5. ITU Telecom World Konferencia 2015

Az ITU rendezvényeinek helyszínét átlátható pályázati eljárás keretében választja ki, a fogadó ország pénzügyi kötelezettségvállalást tesz arra, hogy a rendezvények többletbevételre bízatosítanak. Fontos elv, hogy a földrajzi rotáció is érvényesüljön, valamint a kiállítók és résztvevők számára is elérhető és megfizethető legyen a konferencia.³¹ Hazánk a közép-európai digitális gazdaságban kiemelt szerepet tölthet be, az egyik legjobb telekommunikációs hálózattal rendelkezik Európában,³² és néhány területen élen jár az IKT-iparban, ezek is hozzájárultak ahhoz, hogy az ITU 2015-ös konferenciájának 2015. október 12–15. között a házigazdája lehett. 2014-ben, Katarban kapta meg hazánk a rendezési jogot, melyet aztán a Kormány és az ITU szerződésben, majd azt törvényben is rögzítették.

A konferencia aktuális témáira és az egyesület tagországai előtt álló legfontosabb kihívásokra már a nyitóbeszéd alapján következtethettünk. Az ITU főtitkára köszöntőjében kiemelte, hogy a korábbinál nagyobb intenzitással kívánja ösztönözni a kis- és középvállalatokat az IKT-szektorban történő szerepvállalására, mivel a tudásalapú gazdaságban számos lehetőség rejlik számukra. Kiemelte, hogy a vállalkozók több mint 95 százaléka kis- vagy középvállalkozó, a kvv-szektor a munkaerő mintegy 70 százalékát foglalkoztatja, és a fejlődő országokban ők adják a munkahelyek mintegy 80 százalékát. Ezért egy olyan platformot kíván számukra kialakítani, ahol meg tudják osztani egymással innovatív ötleteiket és hatékonyan együttműködhetnek.³³

Magyarország az ásványkincsek helyett tudástőkéjét kívánja értékesíteni a világpiacon, ehhez kiemelkedő alapként szolgálhat Bolyai Farkas és János, Neumann János, a számítástechnika, vagy Kemény János, a számítógépes programnyelvek atyja, valamint Puskás Tivadar, a telefonhírmondó feltalálója hozzájárultak ahhoz, hogy az infokommunikáció tudománya ma ilyen fejlett lehet hazánkban. E korábbi sikerekre mint szellemi örökségre építve a modern IKT-fejlesztők, vállalkozások is nemzetközi megbecsültséget érhetnek el, emelte ki Orbán Viktor a nyitóbeszédében, majd ismertette a Századvég és az IVSZ hazai IKT-szektor gazdasági teljesítményét elemző közös kutatását.³⁴ Kiemelte azokat a törekvéseket is, amelyek a közigazgatás hatékonyságának fejlesztésére irányulnak a telekommunikációs innováció, különösen a széles sávú hálózat fejlesztésével kapcsolatban.

A szektorokon átívelő partnerségek és újdonsült együttműködési formák jelentőségét emelte ki Karas Mónika, az NMHH elnöke nyitóbeszédében. Szerinte a technológiai fejlődés és az új megoldások napról napra újradefiniálják az iparágat: az 5G-re épülő jövőbeli

31 Lásd Magyarország Kormánya és a Nemzetközi Távközlési Egyesület között az ITU Telecom World 2015 konferencia megrendezéséről, megszervezéséről és finanszírozásáról szóló megállapodás kihirdetéséről szóló 2015. évi LXVIII. törvényt

32 Kerstin GUNTER: *Opening Speech ITU Telecom World 2015*, 2015. 10. 12. Forrás: www.youtube.com/watch?v=IRW39sLdOBs (2016. 01. 04.)

33 Speech by ITU Secretary-General, Houlin ZHAO: *ITU Telecom World 2015: Opening Remarks*. Forrás: www.itu.int/en/osg/speeches/Pages/2015-10-12.aspx (2016. 01. 04.)

34 ORBÁN Viktor beszéde az ITU Telecom World 2015 konferencián. Forrás: www.kormany.hu/hu/a-miniszterelnok/beszedek-publikaciok-interjuk/orban-viktor-beszede-az-itu-telecom-world-2015-konferencian (2016. 01. 04.)

mobilkommunikációs technológia kialakítása, a szabályozási kihívások, az IoT (dolgok internete) és a felhő-megoldások folyamatos fejlődése várható a közeljövőben.³⁵

A magyar sikerekben is kulcsszerepet játszanak a kis- és középvállalkozások, mind a köztársasági elnök, mind a nemzeti fejlesztési miniszter nevesítette ezeket.³⁶ Áder János szerint hazánk célja, hogy legalább 300 tudásalapú, intenzív növekedésű magyar kkv lépjen be a globális piacra 2020-ra, és emellett legalább 1000 innovatív startup cég jöjjön létre a következő időszakban.

A konferencia keretében rendezett gazdasági miniszterek ülésén elfogadták a Budapest Akciótervet, amely a tavaly Dél-Koreában, Busánban rögzített Connect 2020 Agenda megvalósításának felgyorsítását tűzi ki célul. A busani nyilatkozat legfontosabb céljai között szerepelt, hogy 2020-ra a háztartások 55 százalékának legyen internet-hozzáférése, illetve hogy az emberek 60 százaléka legyen internet-használó,³⁷ ami elősegíti újabb piacok nyitását és a felhőalapú technológiák elterjedését.

A kkv-k és a kormányzatok közötti együttműködés kérdéseit fejtegette a konferencia második napján tartott panelbeszélgetés is.³⁸ Az ITU képviselője emlékeztette a résztvevőket, hogy jelenleg az IKT-szektor különböző technológiák, nézetek és szereplők komplex rendszere, melyben a tagok önmagukban gyengék, azonban együttesen nagy gazdasági erővel bírnak, ezt bizonyítja az a tény is, hogy a fejlődő országokban a foglalkoztatottak mintegy 80%-a ebben a szektorban tevékenykedik.

Az üzleti szféra résztvevői, bár más-más régiókat képviseltek, egyhangúan kijelentették, hogy a vállalkozások és a kormányok közötti együttműködés legfontosabb kérdése, hogy a kormánytagoknak meg kell érteniük a szóban forgó kérdéseket, és meg kell győződniük a technológia nélkülözhetetlen szerepéről. Ha a kormányok és az üzleti szféra között a kommunikáció nyílt, akkor a kormányok vezetői meg tudnak győződni arról, hogy a kkv-szektorban milyen szükségletei vannak, így nem csak a megfelelő infrastruktúra kerül kiépítésre, hanem létrejön egy olyan környezet, amely a vállalkozások számára folyamatos növekedést biztosít.

A panelbeszélgetés során a szereplők kihangsúlyozták a nemzeti vállalatokat védő szabályozás fontosságát. Kiemelték, hogy az innovatív megoldások egy gyorsan változó, dinamikus, információalapú környezetben jönnek létre, így szükséges, hogy a Kormány megossza a rövid, közép- és hosszú távú terveit az üzleti szférával.

A konferencia harmadik napjának kiemelkedő eseményén a Big Data felhasználásának kormányzati működésre gyakorolt hatását fejtegették.³⁹ Az egészségügytől a közlekedéstervezésig, a katasztrófaelhárítás, a mezőgazdaság, az élelmiszeripar, alig van olyan terület, ahol

35 NMHH: *Egy új digitális kor felé tartunk az infokommunikációs szektor fejlődésével*. Forrás: nmhh.hu/cikk/168370/NMHH_Egy_uj_digitalis_kor_fele_tartunk_az_infokommunikacios_szektor_fejlodesevel (2016. 01. 06.)

36 SESZTÁK Miklós szerint „Az innováció az a híd, amely a jövővel összeköt minket, ez a rendezvény pedig még inkább összekapcsolja majd a magyar startup és más IKT-szektorban működő vállalatokat a világgazdasággal”.

37 *Infokommunikációs vállalkozások ezreit segíti a kormány*. Forrás: www.infoter.eu/cikk/infokommunikacios-vallalkozasok-ezreit-segiti-a-kormany (2016. 01. 04.)

38 ITU 2015 Highlights: *Government and SME Dialogue*. Forrás: <http://telecomworld.itu.int/daily-highlights-2/government-and-sme-dialogue/> (2015. 12. 01.)

39 ITU 2015 Highlights: *Data rich, decision making poor – how to use big data for improved government action*. Forrás: telecomworld.itu.int/daily-highlights-3/data-rich-decision-making-poor/ (2015. 12. 01.)

a kormányzat ne tudná az összegyűjtött adatokat felhasználni. A panelbeszélgetés résztvevői kifejtették, hogy a megfelelő döntések meghozatalához jó minőségű adatokra van szükség. A fejlődő országokban a hagyományos statisztikai és adatgyűjtési módszerek nem tudnak megfelelően működni, a begyűjtött információ gyakran hiányos, rossz minőségű.

Az esemény utolsó napja a Next Generation Day, az ITU történetében egyedülálló módon megrendezett nyílt nap volt, melyen a magyar egyetemisták és fiatal vállalkozók térítésmentesen tekinthették meg a kiállítást. A Nemzeti Közszolgálati Egyetem hallgatóit leginkább a Smart City megoldások (könnyű szerkezetű busz, intelligens menetrendjelző tábla) és hétköznapiabb fejlesztések, például egy digitális vezérlésű, alvást segítő maszk hozta lázba.

A kiállításon 283 kiállító pavilonjait – köztük a tagállamok és multinacionális IT-vállalatok legújabb innovációit rejtőket – tekinthették meg az érdeklődők.⁴⁰ Az ITU Távközlés Fejlesztési Irodájának „Okos IKT a Fenntartható Fejlődésért” nevű pavilonja a kiállítótér középpontja volt, szakmai és ismeretterjesztő előadásokkal és programokkal, előadásokat hallgathattak például a mezőgazdaságba szánt IT-eszközökről, az e-egészségügyi fejlesztésekről, okosvárosokról és drónokról, valamint a biztonságos és felhasználóbarát digitális fizetési szolgáltatásokról. Észtország képviselői az e-közigazgatás területén elért sikereikről számoltak be, bemutatták, hogyan működik teljesen digitálisan, papírtmentesen a Kormány Kabinet. Egyiptom képviselői a fogatékkal élő személyek számára nyújtott IKT-fejlesztéseket ismertették.

A kiállítótér központi eleme, a Magyar Nemzeti Pavilon, a piac legfontosabb hazai szereplői és számos kkv számára nyújtott bemutatkozási lehetőséget. Jelen volt az MVM Csoport, a Nemzeti Mobilfizetési Zrt., a NISZ Zrt., és számos további szabályozott elektronikus ügyintézési szolgáltatást nyújtó intézmény, de a hazai egyetemek (pl. ELTE, BME, SZIE) is képviseltették magukat a rendezvényen.

Az ITU '15 konferencia megrendezése minden tekintetben hazánk versenyképességének növekedését szolgálja. Kapcsolatépítési fórumként és inspiráló erőként hat a hazai IKT-szektor szereplőire, a fiatal generációra, a jövő kutatóira és vezetőire egyaránt. Reméljük, hogy a rendezvényen elhangzott előadások és a nemzetközi kitekintés segíteni fogja az EU és hazánk digitális megújulást célzó programjait, az e-közigazgatási megoldások terjedését, valamint az ITU mottójának megvalósítását: „Better, sooner” azaz a munkánkat végezzük jobban, gyorsabban.



SUMMARY IN ENGLISH: The rapid growth of the ICT sector and its impact on the national and EU level economy can be easily measured. It is the responsibility of the stakeholders and legislators (ITU, EU and Hungary) to enhance innovation, telecommunication development, and the efficiency of electronic services. In our digitalised world we are witnessing a growing number of innovations affecting communication. In 2015 the ITU Telecom World Conference brought together hundreds of ICT-sector professionals, developers and companies in Budapest. This article gives glimpses of the organization's 150th anniversary conference.

⁴⁰ ITU Telecom World 2015 Post Event Report. Forrás: telecomworld.itu.int/wp-content/uploads/2015/11/post_event_2015_report.pdf (2015. 12. 01.)

Beláz Annamária (belazannamaria@gmail.com): a Nemzeti Közszerológálati Egyetem Közigazgatás-tudományi Kar közigazgatási MA, valamint az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar jogász szakos hallgatója. Harmadik éve az E-közszológálati Fejlesztési Intézet demonstrátora. Tudományos tevékenységét az NKE E-közszológálati Tudományos Diákkör titkárhelyetteseként folytatja. Az elmúlt években többek között részt vett e-learning rendszerek fejlesztésében és tesztelésében, illetve európai uniós finanszírozású projektek kidolgozásában. Főbb érdeklődési és kutatási területei: adatvédelem, információbiztonság, médiajog, e-közszológálat és digitális írástudás-fejlesztés.

Dr. Kiss Attila (Kiss.Attila@uni-nke.hu): egyetemi tanársegéd, infokommunikációs szakjogász, a Nemzeti Közszerológálati Egyetem Közigazgatás-tudományi Karának oktatója. Jogász diplomáját 2011-ben, szakjogász oklevelét 2014-ben szerezte a Pécsi Tudományegyetemen. 2011 és 2014 között a Pécsi Tudományegyetem Állam- és Jogtudományi Kar Informatikai és Kommunikációs Jogi Tanszékének nappali tagozatos doktorandusza, a Tanszék kutatóintézetének tagja, 2012 óta az Infokommunikáció és Jog című szakmai lap szerkesztője. 2014 szeptembere óta az NKE KTK E-közszológálati Fejlesztési Intézet Információbiztonsági Tanszékének tagja, az infokommunikációs jogi témák mellett az információbiztonsággal kapcsolatos hazai és nemzetközi jogi szabályozást tanítja alap-, mester-, és szakirányú továbbképzéseken. Kutatási területe elsősorban a személyes adatok és a képmás védelme, több tanulmánya vizsgálja az Európai Unió adatvédelmi reformját.

Szerzőinkhez

A Nemzeti Közzolgálati Egyetem kiadásában megjelenő Pro Publico Bono – Magyar Közigazgatás című szakmai, tudományos folyóirat közigazgatási témájú, tudományos írások közlésére kíván publikálási lehetőséget biztosítani.

A lap célja: a közigazgatás, a közmenedzsment és a közpolitika fejlődését szolgáló lektorált kutatások és szakmai tapasztalatok közlése, a tudományos nézetek és a gyakorlati megfontolások közötti kölcsönhatás erősítése, a közigazgatás minőségének fejlesztését szolgáló tudás közvetítése.

A SZERKESZTŐSÉG AZ ALÁBBI ROVATOKBA VÁR ÍRÁSOKAT:

Tudományos közlemények/Tanulmányok

E rovat célja az államtudomány, jogtudomány és társadalomtudományok területén elért hazai és nemzetközi kutatási eredmények bemutatása, tudományos műhelyek, iskolák eszmecsereje.

Szakmai fórum

E rovat célja teret adni a közigazgatási praxis művelői közötti a tapasztalatcserének, a jó gyakorlatok bemutatásának és a közzolgálat változásait bemutató tudósításoknak.

Nemzetközi kitekintés

E rovat célja a nemzetközi állam- és társadalomtudományi kutatások közvetítése, különösen tudósítani a külföldi közigazgatási stratégiákról és gyakorlatokról, az európai közigazgatási rendszerek közeledéséről és együttműködéséről, az EU törekvéseiről és a nemzetközi szervezetek közigazgatás-fejlesztési programjairól.

Szemle

E rovat tudósít az államtudományok, az államélet és benne a közigazgatás világának szakmai és tudományos eseményeiről, híreiről, programjairól, recenziókat és konferenciabeszámolókat közöl.

MEGJELENÉS

A folyóirat negyedévente jelenik meg nyomtatásban magyar nyelven. A tartalomjegyzék angol, német és francia nyelven is megjelenik.

A megküldött írások közléséről a szerkesztőbizottság dönt ügyrendjének megfelelően. Az írásról referáló szerkesztőbizottsági tag véleményezés, illetőleg lektori vélemény elkészítése vagy kikérése alapján tesz javaslatot az írás megjelentetésére a Szerkesztőbizottság számára. A lektorálás és véleményezés anonim.

A Pro Publico Bono – Magyar Közigazgatás című folyóirat online formában is megjelenik. Az online változat, benne a korábbi lapszámok archívuma a <http://uni-nke.hu/kutatas/egyetemi-folyoiratok/pro-publico-bono-magyar-kozigazgas/> portálon érhető el.

A részletes közlési feltételek megtekintéséhez, kérjük, látogasson el honlapunkra!

**[http://uni-nke.hu/kutatas/egyetemi-folyoiratok/
pro-publico-bono-magyar-kozigazgas/kozlesi-feltetelek](http://uni-nke.hu/kutatas/egyetemi-folyoiratok/pro-publico-bono-magyar-kozigazgas/kozlesi-feltetelek)**

Table of contents

Foreword/Preface	ANDRÁS NEMESLAKI	2
Scientific publications/ Studies	ANDREA KŐ – ZOLTÁN SZABÓ	
	• Innovative e-healthcare solutions – internet technologies of the future in remote monitoring	6
	SÁNDOR RÉPÁS – ISTVÁN DALICSEK	
	• Methodological issues of information security risk analyses in cases of organizations operating critical infrastructural elements	22
	PÁL MICHELBERGER – SÁNDOR DOMBORA	
	• The role of user's profile in information security	34
	ANNA ORBÁN	
	• Customer satisfaction as one of the dimensions of effectiveness	51
	ANDRÁS BENCSIK – ADRIÁN FÁBIÁN – EMESE PÁL – GERGELY LÁSZLÓ SZŐKE	
	• The interface between public administration and the media	60
	ANDRÁS NEMESLAKI – PÉTER SASVÁRI	
	• A felhőalapú számítástechnika használata a köz- és üzleti szférában	76
Professional Forum	VERONIKA NAGYNÉ TAKÁCS – LÁSZLÓ KOVÁCS	
	• Partial experience of specific training for leaders of information security	85
	ZSOLT ORBÁN – PÉTER BALKÁNYI	
	• Challenges and success in mass application of video-based teaching materials	100
	GÁBOR TÖRLEY – PÉTER SASVÁRI	
	• Scientific visibility of researchers of Hungarian public administration	112
International Scope	LILLA MÁRIA JUHÁSZ – CSILLA PAKSI-PETRO – PEDRO REIS	
	• Virtual learning all over the World (Good practice from Portugal)	133
Review	ATTILA KISS – ANNAMÁRIA BELÁZ	
	• Efforts made in the regulation and standardization in the world of ICT and telecommunication.	
	Report of the results and background of ITU Conference 2015.	146

Sommaire

Introduction/Préface	ANDRÁS NEMESLAKI	2
Études	ANDREA KŐ – ZOLTÁN SZABÓ	
	• Solutions électroniques innovantes en santé – les technologies de surveillance à distance pour l'Internet du futur	6
	SÁNDOR RÉPÁS – ISTVÁN DALICSEK	
	• Questions méthodologiques de l'analyse de risqué en cybersécurité – les organisations du secteur des facilités essentielles	22
	PÁL MICHELBERGER – SÁNDOR DOMBORA	
	• La rôle d'un profil utilisateur en cybersécurité	34
	ANNA ORBÁN	
	• La mesure de la satisfaction client; un dimension de l'efficacité	51
	ANDRÁS BENCSIK – ADRIÁN FÁBIÁN – EMESE PÁL – GERGELY LÁSZLÓ SZŐKE	
	• L'interface entre l'administration publique et la mass media	60
	ANDRÁS NEMESLAKI – PÉTER SASVÁRI	
	• L'utilisation du cloud computing dans le secteur public et le secteur privé	76
Forum	VERONIKA NAGYNÉ TAKÁCS – LÁSZLÓ KOVÁCS	
	• Leçons tirées de la formation professionnelle pour Responsable sécurité des systèmes d'information	85
	ZSOLT ORBÁN – PÉTER BALKÁNYI	
	• Des défis et réussites du cyberapprentissage	100
	GÁBOR TÖRLEY – PÉTER SASVÁRI	
	• Les chercher Hongroise d'administration publique et leur visibilité scientifique	112
Perspectives internationales	LILLA MÁRIA JUHÁSZ – CSILLA PAKSI-PETRO – PEDRO REIS	
	• Le cyberapprentissage dans le monde (bonne pratique du Portugal)	133
Revue	ATTILA KISS – ANNAMÁRIA BELÁZ	
	• La réglementation et normalisation des TIC et des télécommunications: rapport sur l'arrière-plan et des résultats de la conférence de l'UIT 2015	146

Inhaltsverzeichnis

Begrüßung	ANDRÁS NEMESLAKI	2
Studien	ANDREA KŐ – ZOLTÁN SZABÓ	
	• Innovativ e-Lösungen im Gesundheitswesen – Internet Technologien der Zukunft in dem Fernmonitoring	6
	SÁNDOR RÉPÁS – ISTVÁN DALICSEK	
	• Methodologische Fragen der Risikoanalyse in der Informationssicherheit bei den kritische infrastrukturelle Elemente betreibenden Organisationen	22
	PÁL MICHELBERGER – SÁNDOR DOMBORA	
	• Die Rolle der User-Profile in der Informationssicherheit	34
	ANNA ORBÁN	
	• Die Kundenzufriedenheit – als Dimension der Effektivität	51
	ANDRÁS BENCSIK – ADRIÁN FÁBIÁN – EMESE PÁL – GERGELY LÁSZLÓ SZŐKE	
	• Querschnitte zwischen der Verwaltung und den Medien	60
	ANDRÁS NEMESLAKI – PÉTER SASVÁRI	
	• Der Gebrauch der „cloud“ Informatik in der öffentlichen und der Geschäftssphäre	76
Fachforum	VERONIKA NAGYNÉ TAKÁCS – LÁSZLÓ KOVÁCS	
	• Teilerfahrungen des Spezialfortbildungskurses „Leiter für Informationssicherheit“	85
	ZSOLT ORBÁN – PÉTER BALKÁNYI	
	• Erfolge und Herausforderungen bei der massenhaften Anwendung der Video-Unterrichtsmaterialien	100
	GÁBOR TÖRLEY – PÉTER SASVÁRI	
	• Die wissenschaftliche Sichtbarkeit der ungarischen Verwaltungsforscher	112
Internationaler Ausblick	LILLA MÁRIA JUHÁSZ – CSILLA PAKSI-PETRO – PEDRO REIS	
	• Virtuelles Lernen auf der Welt (Gut Praxis aus Portugal)	133
Rundschau	ATTILA KISS – ANNAMÁRIA BELÁZ	
	• Regelung- und Vereinheitlichungsbestrebungen in der Fernmeldetechnik und in der IKT. Bericht über die Ergebnisse der ITU Konferenz 2015.	146

Impresszum

PRO PUBLICO BONO – MAGYAR KÖZIGAZGATÁS

KIADÓ: NKE Szolgáltató Nonprofit Kft.

A KIADÁSÉRT FELELŐS: Hegyesi József

A SZERKESZTŐBIZOTTSÁG ELNÖKE: Prof. Dr. Kiss György, KTK dékán

FŐSZERKESZTŐ: Dr. Fejes Zsuzsanna, NKE KTK tanszékvezető,
egyetemi docens

OLVASÓSZERKESZTŐ: Kutas Éva

A papíralapon megjelenő kiadvány azonosítószáma: ISSN 2063-9058

Az internetes kiadvány azonosítószáma: ISSN 2063-9066 (online)

Szerkesztőség

SZERKESZTŐSÉGI TITKÁR: Paksi-Petró Csilla, NKE KTK egyetemi tanársegéd

CÍME: Nemzeti Közszolgálati Egyetem, 1118 Budapest, Ménesi út 5.

LEVELEZÉSI CÍM: 1519 Budapest, Pf.: 275

E-MAIL-CÍM: ppb.mk.szerkesztoseg@uni-nke.hu

WEBLAP: <http://uni-nke.hu/kutatas/egyetemi-folyoiratok/pro-publico-bono-magyar-kozigazgatas>

Nyomda

NYOMDAI MUNKA: Séd Nyomda Kft.

FELELŐS VEZETŐ: Katona Szilvia

WEBLAP: www.sednyomda.hu



PRO PUBLICO BONO - MAGYAR KÖZIGAZGATÁS

A NEMZETI KÖZSZOLGÁLATI EGYETEM ÁLLAM- ÉS KÖZIGAZGATÁS-TUDOMÁNYI SZAKMAI FOLYÓIRATA

Tisztelt Olvasó!

A **Pro Publico Bono – Magyar Közigazgatás** szerkesztősége továbbra is várja mind az akadémiai világból, mind pedig a közigazgatás gyakorlati témáit feldolgozó írásokat. A folyóirat célja, hogy a közigazgatási és államigazgatási tudományok fő szakmai tudósítójaként a tudományterületek közötti párbeszédet segítse elő.

Bővebb tájékoztatás érdekében látogasson el a <http://uni-nke.hu/kutatas/egyetemi-folyoiratok/pro-publico-bono-magyar-kozigazgas/> weboldalra, vagy forduljon szerkesztőségünk munkatársaihoz a ppb.mk.szerkesztoseg@uni-nke.hu e-mail-címen!

Bízunk a sikeres szakmai együttműködésben!

Pro Publico Bono!

Dr. Fejes Zsuzsanna
tanszékvezető, egyetemi docens

Prof. Dr. Kiss György
KTK dékán

PRO PUBLICO BONO – Magyar Közigazgatás

A NEMZETI KÖZSZOLGÁLATI EGYETEM ÁLLAM- ÉS
KÖZIGAZGATÁS-TUDOMÁNYI SZAKMAI FOLYÓIRATA

KIADÓ: NKE Szolgáltató Nonprofit Kft.

A SZERKESZTŐBIZOTTSÁG ELNÖKE: Prof. Dr. Kiss György, KTK dékán

FŐSZERKESZTŐ: Dr. Fejes Zsuzsanna,
tanszékvezető, egyetemi docens

A SZERKESZTŐSÉG CÍME: 1118 Budapest, Ménesi út 5.