

JELIGE: HAJNALCSILLAG

E-PRIVACY: „HOT TOPIC” A KÖZIGAZGATÁSBAN?

TARTALOM

BEVEZETÉS	2
HIPOTÉZISEK	3
A DOLGOZAT MÓDSZERTANA	4
I. A PRIVACY FOGALMA ÉS JOGI KERETEI	5
1.1 MAGÁNSZFÉRA VÉDELEM ÉS ADATVÉDELEM KAPCSOLATA	5
1.2 ÁLTALÁNOS ADATVÉDELMI ALAPELVEK	8
1.3 PRIVACY VÉDELEM MODELLJEI	12
II. MIÉRT FONTOS AZ ADATVÉDELEM?	13
2.1 FELMÉRÉS AZ ÁLLAMPOLGÁRI ISMERETEKRŐL: TÉNYEK FEKETÉN FEHÉREN	13
2.2 AZ ISMERET HIÁNYA: SZEMÉLYAZONOSSÁG LOPÁS	15
2.3 AZ ISMERET HIÁNYA: GROOMING	16
2.4 AZ ISMERET HIÁNYA: DEPRESSZIÓ, ÖNGYILKOSSÁG	16
III. MIT TEHET A KÖZIGAZGATÁS A PRIVACY VÉDELEM TERÜLETÉN?	17
3.1 JOGI ÉS INTÉZMÉNYI KERETEK	17
3.2 KÖZOKTATÁS	22
3.3 KAMPÁNYOK, CIVIL SZERVEZETEK ÉS PRIVACY SZAKÉRTŐK	24
3.4 AZ EGYÉN FELELŐSSÉGE	25
KÖVETKEZTETÉSEK	25
MELLÉKLETEK	27
INTERJÚK	27
DR. MAJTÉNYI LÁSZLÓ	27
DR. PÉTERFALVI ATTILA	32
HIDVÉGI FANNY	36
KUTATÁSHOZ HASZNÁLT KÉRDŐÍV	42
JOGFORRÁSOK	44
BIBLIOGRÁFIA	46

BEVEZETÉS

*„A világ változik, és mostanában egyre gyorsabbak a változások.
Felgyorsult a tempó, és ezt ki kell használni.
Új horizontok nyílnak.”*
Agatha Christie

Az online média: fiatalos, lenyűgöző, újszerű, rejtélyes, hatásos, forradalmi, az „életünk része”. A Facebook több mint egy milliárd felhasználója, Kína és India után, a világ harmadik legnagyobb államát alkotja. A közösségi média használata elsősorban a webes szolgáltatások közül, még úgy is, hogy a legnagyobb közösségi oldalak és keresőmotorok (Facebook, Twitter, Google, YouTube) Kínában be vannak tiltva. Az online életünk hatással van az interperszonális kapcsolatainkra is: statisztikák szerint minden ötödik vásárlásért a Facebook hibáztatható. Minden percben 72 órányi videó anyagot töltenek fel a YouTube videó megosztó portálra. A Wikipedia nevű Internetes lexikon könyvformátumba 2,25 millió oldalt tenne ki. Lady Gagának, Justin Biebernek és Katy Perrynak több követője van twitteren, mint Németország, Törökország, Dél-Afrika, Kanada, Argentína vagy Egyiptom teljes népessége.¹

Az online média: veszélyes. Egy kereskedelem és információ alapú társadalomban élünk, ahol a profitszerzés a mindennapok mozgatórugója. Mindenhol ugyanazt akarják tőlem: Információt. Magamról. Önként. Kitöltöm az űrlapokat, és közben abban reménykedek, hogy nem fognak visszaélni az adataimmal, mert tudom a 25%-os kedvezményre jogosító kártyát nem adják ingyen. Manapság már nem az a legfőbb félelem, hogy megtámadnak az utcán, vagy betörnek a lakásunkba és elviszik az értékeinket. Miért is lopnák el a tárgyainkat, ha valami sokkal értékesebbet is elvihetnek? Jogosan merül fel a kérdés: Teljesen védtelenek vagyunk, egy az egész világot behálózó adatháború közepén?

Az online média: lehetőség. Ahogyan Agatha Christie is megfogalmazta a változások egyre gyorsabban mennek végbe a modern világunkban, de ez közel sem jelenti azt, hogy a változásoknak csak negatív hatásait érezzük. Folyamatosan új lehetőségek nyílnak meg, a lehetőségekkel pedig élni kell. Nem csupán az egyes embereknek kell adaptálódniuk az új információs társadalmi környezethez, hanem az államok közigazgatási rendszerének is, mivel a sikeres alkalmazkodás következtében kiszűrhetők a veszélyforrások, javulhat a kapcsolat az állam- állampolgár viszonyban és növekedhet az állampolgárok biztonságérzete.

Az online média: „hot topic”. Vajon a közigazgatásban annak kell lennie?

¹ Részletesebb statisztikáért ld: **QUALMAN** (2012)

Hipotézisek

2013. június 6.-án megrázó riport jelent meg a The Guardian hasábjain. Edward Snowden szerint az amerikai Nemzetbiztonsági Ügynökség (NSA) egy titkos bírósági döntésre hivatkozva, több tízmillió amerikai állampolgár telefonbeszélgetéseit hallgatta le. „A kiszivárogtatott dokumentumok szerint az NSA a PRISM fedőnevű rendszer segítségével a Microsoft, a Google, a Yahoo, a Facebook, a YouTube, a Skype, az AOL, az Apple és a PalTalk internetes óriásvállalatok és szolgáltatások adatforgalmát is megfigyelte.”²

Az infokommunikációs világban, a fejlődő technológiák és eszközök kavalkádjában az egyének visszaéléseknek vannak kitéve. A nagyvállalatok „vadásznak” az emberek személyes adataira, hogy célzott hirdetésekkel, minél több vásárlót minél rövidebb idő alatt megnyerjenek maguknak. E mellett pedig „az államnak az az érdeke, hogy minél többet tudjon... Az öntözéses kultúráktól, az istenkirályoktól egészen napjainkig az államnak alapvető, természetes igénye, törekvése, hogy minél többet tudjon az állampolgáiról. Egyrészt ezt hatékonysági szempontból, de mindenekelőtt hatalmi szempontból lehet indokolni.”³

A közigazgatás számára talán a legnehezebb feladat, hogy egy ilyen gyorsan változó világban is védelmet tudjon nyújtani az állampolgárainak. Egyrészt fontos, hogy az állampolgárok bizalma a közigazgatás felé töretlen maradjon, másrészt a közigazgatásnak meg kell tennie mindent, hogy alkalmazkodni tudjon a globalizálódó világhoz. Az adatvédelem területén ez magába foglalja a jogi szabályozást, a stabil közigazgatási intézményrendszert, valamint a folyamatos képzést és továbbképzést.

Az adatvédelem területén folytatott kutatómunkám kezdetén az alábbi hipotéziseket állítottam fel:

- Az adatvédelem, különös tekintettel az online információk privacy területére kulcsfontosságú kérdés, ezért pontos jogi szabályozást igényel.
- Az állampolgárok általában véve nincsenek tisztában az információk önrendelkezési jogaikkal. Az internetet adatvédelmi szempontból nem használják tudatosan, személyes adataikkal való visszaélés esetén nem tudják, milyen segítséget kaphatnak.

² Az eredeti cikkért lásd: Az NSA milliók telefonbeszélgetéseit gyűjti:
<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> (2014.10.01)
Magyarul megjelent összefoglaló cikk a Snowden- ügygel kapcsolatban:
http://index.hu/kulfold/2013/07/22/minden_ami_snowden/ (2014.10.01)

³ Dr. Majtényi László. A teljes interjút lásd a Mellékletek között.

- Az államnak felelőssége megvédeni állampolgárai jogait, beleértve az információs önrendelkezési jogokat is. Kötelessége felhívni az állampolgárainak figyelmét a személyes adataikkal összefüggésbe hozható veszélyekre, valamint gondoskodnia kell az ezek elhárításához szükséges ismeretek átadásáról, azaz a képzésről. (Az állampolgárok számára az adatvédelem területén nyújtott állam általi képzést, oktatást a továbbiakban ügyfélképzésnek nevezem.)

Dolgozatom célja, hogy - miközben feltárom a hazai adatvédelmi jog, a közigazgatás és az ügyfélképzés területén fennálló hiányosságokat- alátámasszam a megállapításaimat, és gyakorlati megoldási modelleket vázoljak fel.

A dolgozat módszertana

A kutatásom során az információs privacy területét vizsgáltam meg. Dolgozatom első fejezetében átfogó jelleggel bemutatom a magánszféra védelem és az adatvédelem fogalmát, jogi és elvi alapjait. Kitérek a legfontosabb nemzetközi privacy témájú jogforrásokra is, valamint bemutatom a különbséget az európai és az angol-szász privacy modellek között.

Dolgozatom második fejezetében érveket hozok fel az e-privacy területének fontosságára. Kérdőíves kutatást végeztem, melynek célkeresztjébe az állampolgárok adatvédelmi ismereteit helyeztem, eredményeimet összevetem a Nemzeti Adatvédelmi és Információszabadság Hatóság kutatási eredményeivel, majd megtörtént eseteket vázlok fel, melyek az ismeretek hiányára és a veszélyek evidenciájára irányítják a figyelmet.

A harmadik fejezet a közigazgatás felelősségét és szerepét tárgyalja a privacy védelem kérdésében. Kitérek a jogalkotás, az intézményrendszer, az ügyfélképzés, valamint egyéb figyelemfelhívó eszközök használatára. Ezen kívül górcső alá veszem a szakértők, a civil szervezetek nem utolsó sorban az egyének szerepét a privacy védelem tárgykörében.

Annak okául, hogy a témakörömben, teljes mértékben el tudjak mélyedni valamint, hogy adekvát álláspontokat mutassak be, három mélyinterjút készítettem. Az interjúk a dolgozat átfogó megértését szolgálják, fontos jogi kérdéseket boncolgatnak. Teljes szövegű változataik a dolgozat mellékletei között találhatóak meg.

Interjúalanyaim:

- Dr. Majtényi László (a Magyar Köztársaság első adatvédelmi biztosa, jelenleg a Magyar Tudományos Akadémia doktora, az Eötvös Károly Közpolitikai Intézet elnöke)

- Dr. Péterfalvi Attila (a Magyar Köztársaság adatvédelmi biztosa, jelenleg a Nemzeti Adatvédelmi és Információszabadság Hatóság elnöke)
- Hidvégi Fanny (jogász, a Társaság a Szabadságjogokért civil szervezet adatvédelmi és információszabadság programvezetője)

I. A PRIVACY FOGALMA ÉS JOGI KERETEI

Az adatvédelem kifejezés meggyökeresedett a világ nagy jogrendszereiben (lásd: data protection, datenschutz, protection des données, protección de datos), mégis elmondhatom, hogy ez a kifejezés pontatlan. Az adatvédelem nem a konkrét adatoknak a védelmét (például egy személy etnikai hovatartozására vonatkozó adat védelmét jelenti, ezt ugyanis az adatvédelem kérdéskörében adatbiztonságnak nevezzük), hanem magának az adatalánynak (másképpen: a személynek, az élő embernek) a védelmét jelenti. Ezért a továbbiakban a magánélet, magántitok és személyes adatok védelmének kifejezésére előnyben részesítem az angol-szász területen ismert privacy védelem, pontosabban az információs privacy (vagy e–privacy) védelem kifejezés használatát.

A brit Calcutt Committee 1990-ben adta a privacy egyik legpontosabb meghatározását: „The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.”⁴

1.1 Magánszféra védelem és adatvédelem kapcsolata

Az Emberi Jogok Egyetemes Nyilatkozata 12. Cikk a következőket mondja:

„Senkinek a magánéletébe, családi ügyeibe, lakóhelye megválasztásába vagy levelezésébe nem szabad önkényesen beavatkozni (...) Minden személynek joga van az ilyen beavatkozásokkal, vagy sértésekkel szemben a törvény védelméhez.”

Az Emberi Jogok Európai Egyezményének 8. cikke pedig az alábbi rendelkezést tartalmazza:

„Minden embernek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság, vagy az ország gazdasági jóléte érdekében, zavargás, vagy bűncselekmény

⁴ Report of the Committee on Privacy and Related Matters, Cm. 1102 (1990) In: **MCELDOWNEY** (1998) pp. 642-643

Fordítás: Az egyén joga arra nézve, hogy védelmet élvezzen a személyes- és családi életébe, illetve a magánügyibe való illetéktelen behatolás alól, legyen az fizikai értelemben vett, vagy a személyes adatainak nyilvánosság elé terjesztése által.

megelőzése, a közegészség, vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.”⁵

Ezek a cikkek általánosságban beszélnek a magánszféra védelméről, azonban dolgozatomban a magánszféra védelem egy szűk területére, az információs önrendelkezési jogokra (másképpen az egyén joga ahhoz, hogy kontrollt gyakorolhasson a róla szóló adatok felett) koncentrálok. Úgy vélem minden emberben meg van a természetes vágy, hogy a személyünkről szóló információkat, csak az általunk kiválasztott személyek ismerhessék meg.

A mindennapi életben is természetes, ha a kórházban fekvő magatehetetlen családtagunkat látják az orvosok, a nővérek, a kórházi alkalmazottak, de semmiképpen sem kívánnánk, ha a családtagunkról ilyen állapotban készült fénykép a napilapok címlapján szerepelne.⁶

Esetenként azonban előfordul, hogy ezek az információk napvilágot látnak. A telefonos lehallgatások, a biztonsági kamerák használata manapság egyre elterjedtebbé válik. A pontos helyzetünk egyszerűen meghatározható a mobiltelefonjaink által folyamatosan közvetített GPS koordinátáknak köszönhetően. Ezek az eszközök egyre nagyobb fenyegetést jelentenek a magánélet védelméhez való jogra nézve.

Az e-privacy védelme az emberi szabadság és méltóság alapvető értéke. Sokkal méltóságteljesebb és nyugodtabb életet élhetünk, ha a mindennapokban nem kell azon aggódnunk, hogy nyilvánosságra jutnak az életünk azon területei, amelyeket mi inkább titokban tartanánk.⁷ Napjainkban a biztonság fejlesztésének tipikus módja a nemzetközi tele- és Internet alapú kommunikáció fejlődésének lekövetése. A repülőtéri biztonsági ellenőrzés például hihetetlenül magas szintű. Beléptető kapuk rendszere, átvilágítások, kamerák, megfigyelés... A biztonsági ellenőrzések ily magas szintje felvet egy következő kérdést? Megvalósulhat valaha az utópia, hogy az orvosok az agyfunkcióink elemzésével a gondolataink feltárására vállalkoznak?⁸ Meddig terjed az egyén magánszférájának védelme?

A modern állam funkcióinak növekedése fokozatosan megkövetelte egyre több adat nyilvántartását és kezelését. A számítástechnika fejlődésének köszönhetően az adatkezelés és feldolgozás könnyebbé és gyorsabbá vált, azonban az adatok mennyiségének növekedésével

⁵ Convention for the Protection of Human Rights and Fundamental Freedoms CETS No.: 005 <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm> (2014.03.29)

⁶ Érdekes, hogy pontosan ez az esemény történt 1991-ben Nagy-Britanniában *Kaye v Robertson & Sport Newspapers Ltd* ügyben. *Kaye v. Robertson* [1991] FSR 62; *The Times* 21 March 1990, *The Independent*, 22 March 1990; *The Guardian*, 22 March, 1990.

SMARTT (2006) pp. 179-180

⁷ **ELLIOTT, THOMAS** (2011) pp. 804-810

⁸ **RAIKKA**, (2010) pp. 5-12

egyenest arányban nőtt az adatokkal való visszaélési lehetőségek száma.⁹ Többek között ezek az okok szolgáltattak alapot arra, hogy az adatvédelem kérdése a jogi szabályozás kiemelkedő tárgyává váljon.

Mielőtt a harmadik generációs jogok megjelenéséről tennék említést, ki kell térnem arra a meglátásra, hogy az általános és nevesített személyiségi jogok minden modern jogrendszer fontos részét képezik, polgári és büntető jogi eredetük azonban egészen a római jog világáig nyomon követhető. Magának a privacy-nak pedig az első megfogalmazása - a híres „right to be let alone” (a jog arra, hogy magunkra hagyjanak) - a XIX. század végéhez, Samuel Warren és Louis Brandeis nevéhez kötődik.¹⁰

Az információs önrendelkezési jogok (a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog) a harmadik generációs jogokhoz, azon belül pedig a személyi szabadságjogokhoz tartoznak. Hogy miért személyi jogok? „A technikai fejlődés eredményeként az emberekről egyre több adatot, egyre könnyebben és olcsóbban tartanak nyilván. Az egyén kapcsolatai jelentős részében nem fizikailag, hanem a rá vonatkozó adatok formájában van jelen. Az ezeknek az adattoknak a kezelésére vonatkozó szabályok megtartása, így végső soron az adatok mögött rejlő *személyiség védelmét* szolgálja.”¹¹ Jelentőségük kettős: egyrészt meggátolják, hogy az állam, a közigazgatás által nyilvántartott adatok a személlyel egyértelműen összekapcsolhatóak legyenek, másrészt az egyén privacy védelmének leghatékonyabb eszközeként funkcionálnak. Sajátosságuk, hogy nem csak az állam-állampolgár közötti jogviszonyokban, hanem szinte minden magánjogi jogviszonyban is érvényesülniük kell.

A privacy védelem összefoglalva tehát „beismerést és elismerést jelent. Annak elismerését, hogy tudjuk, az emberi lényeknek van személyiségük, de beismerjük, hogy nem tudjuk azt a jogban meghatározni. Viszont mivel képesek vagyunk felismerni a személyiség megnyilvánulásait, ezeket a megnyilvánulásokat a nevesített és általános személyiségi jogokkal, illetve a személyes adatok védelmének eszközeivel viszonylag hatékony védelemben részesíthetjük.”¹²

⁹ SÁRI, SOMODY (2008) pp133-141

¹⁰ BRANDEIS, WARREN (1890)

¹¹ SZABÓ (2005)

¹² MAJTÉNYI (2010) p. 35

1.2 Általános adatvédelmi alapelvek

Nehéz feladat általános elveket felállítani a privacy védelem területén, hiszen az Európai és az Angol-szász szabályozás rendszere más elvekre és gyakorlatra épül. Míg az európai gondolkodás központjában az emberi méltóság áll, addig az USA alkotmányos szabályozásának legfontosabb értéke az emberi szabadság. Ezzel összefüggésben az európai adatvédelmi szabályzás a nyilvánosság feletti kontrollt helyezi előtérbe, az USA megoldása viszont az otthon szentségén alapul.¹³ Az USA alkotmánya közvetlenül nem nevesíti a magánélet védelméhez való jogot, bár a norma szövege több helyen érinti a magánélet különböző szegmenseit.¹⁴ Többek között:

- 1) szólás-, sajtó- és vallásszabadság (I. alkotmány kiegészítés)
- 2) megalapozatlan házkutatás elleni védelem (IV. alkotmány kiegészítés)
- 3) magántulajdon szentsége (V. alkotmány kiegészítés)¹⁵

A privacy védelméhez való jog tehát nem vezethető le közvetlen módon a magánélet védelméhez való alkotmányos jogból - mint a legtöbb európai és a magyar¹⁶ szabályozásban-, azonban megfelelő jogalapi hivatkozással szolgálhatnak a legfelsőbb bírósági döntések (ex: *right to anonymity*: „right to privacy from government surveillance into an area where a person has reasonable expectation of privacy”) valamint a szektoriális jogszabályok.¹⁷ (Kiemelkedő ezek közül az 1974-es Privacy Act, mely lefekteti az adatvédelem általános szabályait.¹⁸)

A részletesen szabályozott információszabadsághoz való joggal¹⁹ szembeállítva, az USA, a privacy védelem szabályozásában folyamatos identitásvarban szenved. Egyrészt a privacy védelme Louis Brandeis-nek és Samuel Warren-nek köszönhetően több száz éves múltra

¹³ WITHMAN (2004)

¹⁴ Érdekes azonban, hogy már a Függetlenségi Nyilatkozat (Declaration of independence, 1776) megfogalmazta a boldogságkereséshez, egyéni boldoguláshoz való jogot (pursuit of happiness). Véleményem szerint ez a jog, vagy cél nem valósulhatna meg a magánélet szentségének figyelmen kívül hagyásával. Összefoglalva megállapítom, hogy bár a normaszövegben nem szerepel ex lege a magánélet védelméhez való jog, implicit módon azonban megjelenik, továbbá az USA joggyakorlata bizonyítja, hogy a privacy védelme kiemelkedő szerepű.

¹⁵ SCHOEMAN (1984) p. 10

¹⁶ Atv Szabadság és Felelősség fejezet VI. cikk vö.: ÁRVA (2013) pp. 118-123

¹⁷ Legfontosabb szektoriális szabályok: APEC Privacy Framework, CAN-SPAM Act, Cable Communications Policy Act, Privacy Protection Act, Intelligence Surveillance Act, HIPAA Regulations Act, Real ID Act

¹⁸ Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579, (Dec. 31, 1974)

¹⁹ The Freedom of Information Act, 5 U.S.C. § 552, Public Law 89- 554, 80 Stat. 383; enacted 4 July, 1966, Amended 1996, 2002, 2007 (a továbbiakban: FIOA)

tekint vissza.²⁰ Másrészt az USA nem rendelkezik általános privacy szabályokkal. A szövetségi információszabadság törvény (FIOA) és a tagállamok információszabadság törvényei egyaránt küzdenek a magánélet védelmének biztosításával, pontosabban a „magánszférába történő jogtalan behatolás”²¹ szabályozásával.

Az EU Bizottsága és az Egyesült Államok képviselői hosszas tárgyalásokat folytattak az adatvédelem szabályozásának megfelelő szintjéről. 1999-ben az EU Bizottság a következő állásfoglalást tette közzé: „Az Egyesült Államok adatvédelemre és magánszféra- védelemre vonatkozó szabályozása a szövetségi és tagállami szabályozás ipari önszabályozással kiegészített bonyolult szövete (...) a(z) [EU adatvédelmi irányelve alapján működő] munkabizottság álláspontja az, hogy a (...) szabályozás nem nyújt minden esetben adekvát védelmet az Európai Unióból továbbított adatok számára.”²²

A tárgyalások eredménye a 2000-ben született úgynevezett Safe Harbor Agreement. A megegyezés szerint az amerikai Kereskedelmi Minisztérium irányításával elindult egy program mely keretében egyes (az EU- irányelveknek megfelelően működő) cégeket az EU elismer olyannak, mintha az azokhoz történő adattovábbítás „megfelelő” védelemmel rendelkező állam területére történne. A programhoz csatlakozó szervezeteknek meg kell felelniük bizonyos alapelveknek (Safe Harbor Principles); az alapelvek érvényesülését az USA hatóságai (különösen a Federal Trade Commission) ellenőrzik.

A 2001. szeptember 11-i terrortámadás következtében az USA adatvédelmi szabályozása sokat szigorodott (terror-ellenes harc magánszféra-védelem szintjére redukálása), manapság nem csak Európa exportálja politikáját az USA-ba, hanem az Államok adatvédelmi szabályozásai túlterjeszkednek a fizikai korlátokon.²³

Az OECD irányelv jelentősége

1981-ben a Gazdasági Együttműködési és Fejlesztési Intézet (OECD) a „fair information principles” (azaz az évtizedek során kialakult „méltányossági információs alapelvek”) alapján részletes irányelveket adott ki.²⁴ Ezen irányelveket az Európa Tanács 1981-ben a személyes adatok számítógépes rendszerekben történő feldolgozásáról szóló egyezményében foglalt

²⁰ Lásd: 10. lábjegyzet

²¹ „An unwarranted invasion of personal privacy” NY Pub. Off. Law, §87 (2) (b).

²² Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, 1999. január 26.

²³ JÓRI (2005) p. 35

²⁴ OECD, *Guidelines Governing the Protection and Transborder Data Flows of Personal Data*, Paris, 1981 <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> (2014.09.01)

össze.²⁵ Az Irányelv kiemelt jelentősége abban rejlik, hogy hidat képez az Európai és az angol-szász szabályozási rendszerek között.

Az OECD irányelvei abból a felismerésből születtek, hogy nem elegendő a magánélet védelmét szolgáló nemzetközi szerződések kidolgozása, hiszen a törvények különbözősége szükségtelenül megakadályozná az információk szabad áramlását. Az információ és a tudás hatalom, ahogyan azt maga Francis Bacon is mondta, s mivel az információ, az adat önmagában gazdasági értékkel rendelkezik, ezért biztosítani kell a tisztességes verseny szabályai szerinti védelmét.²⁶ Az Irányelv alapján az alapelveket két csoportba oszthatjuk aszerint, hogy nemzeti, vagy nemzetközi alkalmazásúak.

A nemzeti alkalmazás követelményei (tágabb értelemben általános adatvédelmi alapelvek)

1) Az adatgyűjtés korlátozásának elve

A személyes adatok gyűjtése csak törvényes és tisztességes eszközökkel, az adatalany tudtával és beleegyezésével történhet.

2) Az adatminőség elve

Az adatoknak felhasználási céljaikkal összhangban és mértékben pontosnak, teljesnek és aktuálisnak kell lenniük. Fontos, hogy ezek a követelmények mindig célhoz kötődnek, tehát sosem terjednek messzebbre, mint az adat felhasználásának és feldolgozásának célja.

3) A célhoz kötöttség elve

Az adatgyűjtés és kezelés megkezdése előtt pontosan meg kell határozni az adatgyűjtés célját. Az így nyert információt csak a cél megvalósulásához szükséges mértékben és ideig lehet felhasználni. Új célokat az adatfeldolgozás során nem lehet önkényesen bevezetni. A cél szempontjából már nem releváns adatok törléséről pedig gondoskodni kell.

4) A korlátozott felhasználás elve

Személyes adatokat felfedni, felhasználni, csak a megjelölt célból lehet, tehát a cél eldönti az adatok felhasználásának lehetőségét. E szabály alól csupán törvényi rendelkezés, vagy az adatalany hozzájárulása nyújthat kivételt.

²⁵ Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, Az egyének védelméről a személyes adatok gépi feldolgozása során című egyezmény, ETS 108, Strasbourg, 1981. Magyarországon kihirdette az 1998. évi VI. törvény <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

²⁶ DIETZ 1995. pp.29-38

5) Adatbiztonság elve

A személyes adatokat a technika mindenkori állásának megfelelő ésszerű biztonsági intézkedésekkel védelmezni kell a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, sérülés és megsemmisülés ellen.

6) A nyíltság elve

Az adatkezeléssel összefüggő tényeket nyíltan kell kezelni. Ennek alapján nyilvános: az adatkezelés ténye, helye, célja, az adatkezelő személye, valamint az adatkezelés politikája.

7) A személyes részvétel elve

Az adatalany megismerheti a rá vonatkozó adatokat, azokat (ha indokolt) helyesbítheti, kiegészítheti, töröltetheti.

8) A felelősség elve

Az adatkezelő felelős az adatvédelmi alapelveknek és a mindenkori jogi szabályoknak megfelelően eljárni, és bizonyítani kell az adatkezelés jogszerűségét. E kötelezettség alól akkor sem mentesül, ha az adatfeldolgozást az ő megbízásából más végzi.

A nemzetközi alkalmazásra vonatkozó ajánlások

- 1) A tagországoknak minden ésszerű és megfelelő intézkedést meg kell tenniük azért, hogy a személyes adatok áramlása zavartalan és biztonságos legyen.
- 2) A tagállamoknak segíteniük kell egymást, hogy az adatok ne veszítsék el a védelmüket, mert más ország területére kerültek.
- 3) El kell kerülniük, hogy a magánélet és a személyes adatok védelmére való hivatkozás ürügyén akadályozzák az információ szabad áramlását.
- 4) A tagállamoknak olyan törvényes eljárásokat kell kidolgozniuk, amelyek eredménye:
 - a) a nemzetközi jog szabályainak megfelelő belföldi törvények
 - b) a gazdasági társaságok önszabályzásának bátorítása
 - c) alkalmas eszközök biztosítása az állampolgároknak jogaik gyakorlásához
 - d) arányos és következetes szankciórendszer kidolgozása
 - e) diszkrimináció tilalmának egyértelmű érvényesülése
 - f) konkrét ügyekben az információcserét és együttműködést biztosító rendszer

1.3 Privacy védelem modelljei

A privacy védelmének négy nagy modelljét különböztetjük meg, ezen modellek nem egymást helyettesítő, hanem inkább egymást kiegészítő, komplementer jelleggel működnek.²⁷ A továbbiakban röviden bemutatom a modellek működésének lényegét.

Átfogó törvények: általános, többfunkciós törvények, melyek szabályozzák a személyes adatok felvételének, kezelésének, továbbításának módját, az állami és a magánszektorban.

Szektoriális törvények: csak bizonyos fajta adatokra, egyes gazdasági ágazatokra terjednek ki. Gyakran olyan területeket ölelnek fel, ahol különleges szabályok és eljárásrendek előírására van szükség például: hitelezés, genetikus információ, elektronikus kereskedelem, az egyének elektronikus megfigyelése, vagy a széleskörű adatgyűjtéssel összefüggő (népszámlálás) szabályozások.

A gazdaság önszabályozó tevékenységének ösztönzése: A szervezetek és gazdasági társaságok működésüket a maguk által elkészített privacy policy alapján szervezik. (Létrehozásukban szerepet játszanak az ágazati magatartási szabályzatok) Az önszabályozással kapcsolatban azonban gyakran felmerülő probléma, hogy a vállalatok nem érdekeltek érdemi adatvédelmi garanciákat biztosítani, hiszen így hátrányos piaci helyzetbe kerülnének, azokhoz a vállalatokhoz viszonyítva, amelyek nem (vagy csak felületesen) szabályozzák tevékenységüket.

Privacy Enhancing Technologie: adatvédelmet és kommunikációs titkosságot biztosító programok és rendszerek, melyek általában encryption-nal (kódolással) segítenek az adatgyűjtés korlátozásában valamint az adatbiztonság megteremtésében. Az Európai Bíróság állásfoglalása²⁸ szerint a PET-ek nem alkalmasak a törvényi szabályozás helyettesítésére, de hasznosak lehetnek a jogszabályok kiegészítéseként.

Összegzésül az adatvédelem (privacy védelem) fogalmát a következőkben határozom meg: Olyan jogi védelem, amely az egyén privacy-jának (magánszférájának) védelmére irányul, az egyénnel összefüggésbe hozható adatok kezelésére vonatkozó eljárási szabályok megteremtésével. Adatvédelmi jogon pedig az ilyen rendelkezéseket tartalmazó jogszabályok összességét értem.

²⁷ BANISAR (2001) pp.9-31

²⁸ 1/98. állásfoglalás: Platform for Privacy Preferences (P3P) és az Open Profiling Standard (OPS), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp11_en.pdf (2014.09.01)

II. MIÉRT FONTOS AZ ADATVÉDELEM?

„Az egyszerű válasz: annyiban vagyunk szabad emberek, amennyiben magánéletünk lehet. Tehát ha a magánéletünket elveszítjük, a szabadságunkat is elveszítjük. Ezért kell az állam és a piac adatéhségével szemben gátakat emelni. Ez a funkciója a személyes adatok védelmének.”²⁹

„Az adatvédelmi szabályozás a magánszféra védelme. Miután a magánszféránál egyre jelentősebb hatása van a digitális adatkezelésnek, ezért az adatvédelem szerepe a technika fejlődésével nem csökken, hanem nő... ma már egy gombnyomással lehet adatokat kezelni.”³⁰

„Az emberek nagy részének még „nem esett le”, hogy a kvázi- ingyenes internetes szolgáltatások úgy működnek, hogy a személyes adataikkal fizetnek érte. Erre a tényre mindenképp fel kell hívni a figyelmet.”³¹

2.1 Felmérés az állampolgári ismeretekről: tények feketén fehéren

A jogszabályokat vizsgálva elgondolkodtam azon, hogy vajon elegendő-e a pontos jogi szabályozás ahhoz, hogy az állampolgárok személyes adatok védelméhez fűződő joga biztosított legyen. Úgy vélem, nem. Ahhoz, hogy a privacy védelem teljes legyen nélkülözhetetlen a felhasználók, azaz az állampolgárok privacy-tudatos hozzáállása.

Ennek a gondolatnak a bizonyítására készítettem egy hat napon át tartó online kérdőíves felmérést.³² A hat nap alatt összesen 201 kérdőív érkezett be. A válaszadók 65%-a 20 és 29 év közötti személy volt, ez azt bizonyítja, hogy sikerült elérnem a célközönségemet. A válaszadóim az egyetemi évfolyamtársaim, a Facebook közösségi oldalon regisztrált ismerőseim, barátaim és tágabb rokonságom köréből kerültek ki. Szerettem volna, hogy a kérdőív olyan személyekhez jusson el, akik rendelkeznek különböző multimédiás eszközökkel, és aktívan használják az internetes közösségi oldalakat, így meg tudom figyelni az online térben megmutatkozó szokásaikat, valamit következtetéseket vonhatok le arra vonatkozóan, hogy mennyire használják privacytudatosan az internetet. Az alábbi ábrákon keresztül néhány fontos eredményt szeretnék bemutatni.

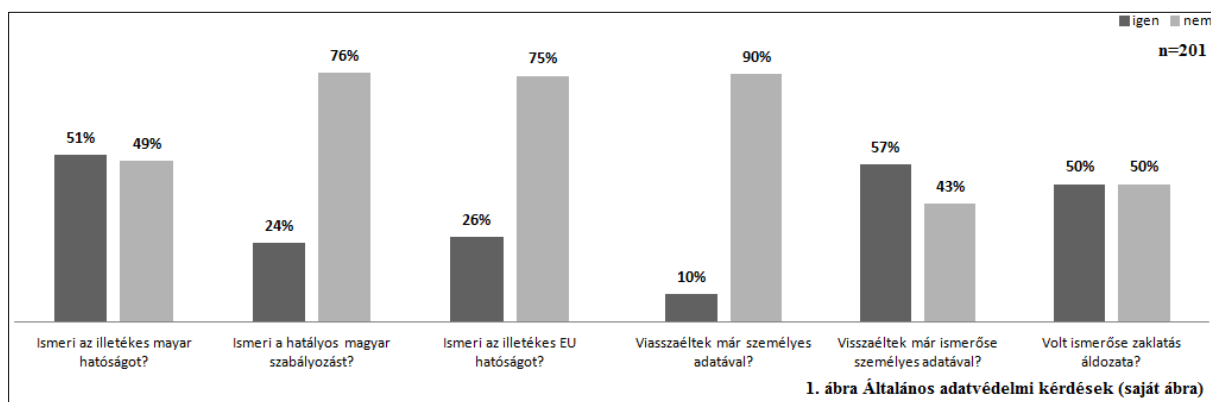
²⁹ Id 3. lábjegyzet

³⁰ Dr. Péterfalvi Attila. A teljes interjút lásd a Mellékletek között.

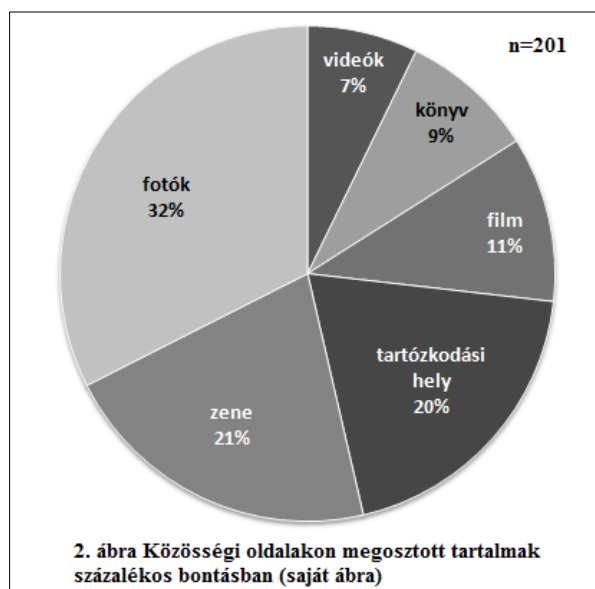
³¹ Hidvégi Fanny. A teljes interjút lásd a Mellékletek között.

³² A kutatáshoz használt teljes kérdőív megtekinthető a mellékletek között. Eredményeimet összevettem a NAIH 2013. február-március hónapban folytatott országos „Az adatvédelem magyarországi helyzetének társadalmi megítélése” című felmérésével. A felmérés a kutatásommal megegyező eredményeket mutat, így a megállapításaimat megalapozottnak tekintem. A NAIH felmérése letölthető a <http://naih.hu/files/adatvedkozvelkut-2013-03.pdf> linkről.

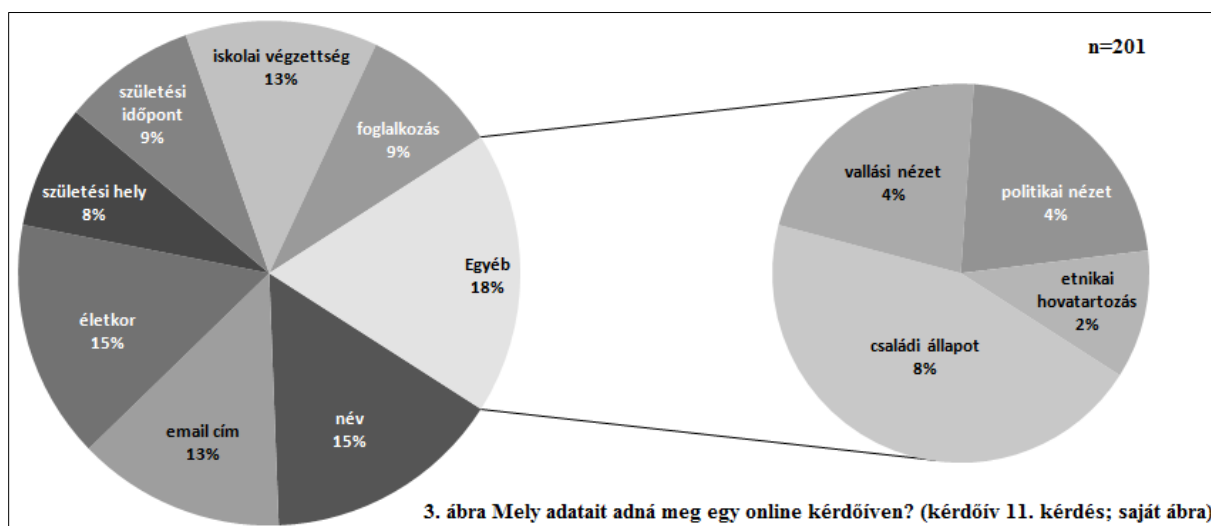
Az 1. ábra (a válaszok százalékos megoszlása) mutatja, hogy válaszadóim, illetve ismerőseik adataival történt-e már visszaélés, valamint jogsértés esetén tudják-e, hogy milyen szervhez fordulhatnak segítségért.



A 2. ábra (a kérdőív 8. kérdésével összefüggésben) bemutatja, hogy válaszadóim milyen információkat osztanak meg magukról rendszeresen (hetente legalább egy alkalommal) az általuk használt közösségi oldalakon.



A 3. ábrán pedig megtekinthető, hogy egy online kérdőíven (amely nem tartalmazza az adatkezelés célját, módját, az adatkezelő személyét) milyen adataikat adnák meg a kérdőívem kitöltői.



Meglepő és figyelemfelkeltő információkhoz jutottam a felmérés által. Számomra a legfurcsább a 3. ábrán az egyéb kategóriába látható adatok voltak. Válaszdóim 2%-a megosztaná etnikai hovatartozását 4-4%-a pedig vallási és politikai nézeteit. Ezek az adataink az úgynevezett szenzitív adatok körébe tartoznak. Ha egy vállalat szeretné bekérni ezeket az adatainkat, akkor írásos nyilatkozatot kell kapnia a beleegyezésünkkel, mely szerint a személyes adatainkat felhasználhatja. Ezzel szemben a legtöbb ember megosztja a közösségi portálokon ezeket a szenzitív adatait, ráadásul nyilvánosan!

Az eredmények azt mutatják, hogy bár a jogi szabályozás adott és megfelelő védelmet nyújtana, az állampolgárok önként lemondanak magánszférájuk védelméről és felelőtlenül használják az internetet, ezáltal visszaéléseknek teszik ki magukat. Mi lehet az oka? Megállapításom szerint elsősorban az ismerethiány valamint az információs társadalmi nyomás. (Ezeket a gondolatokat részletesebben a következő fejezet Közoktatás pontjában fejtem ki, most az ismerethiány okozta problémákra koncentrálok.)

2.2 Az ismeret hiánya: Személyazonosság lopás

„A legtöbben természetesnek vesszük a személyazonosságunkat. Azok vagyunk, akik vagyunk, és ha valaki ezt kétségbe vonja, be tudjuk bizonyítani. De most már olyan könnyű hamisítani vagy ellopni azokat az iratokat, amelyekkel bizonyítani szoktuk a személyazonosságunkat — például a születési anyakönyvi kivonatot, a személyi igazolványt, a jogosítványt, az útlevelet és ehhez hasonló papírokat —, hogy kialakult rá egy bűnözéssel kapcsolatos új szakszó, a *személyazonosság-lopás*.”³³

Ez egy összetett és nehezen lenyomozható bűncselekmény, az áldozatok pedig hirtelen csak azt veszik észre, hogy valaki becsapott másokat és óriási adósságokat halmozott fel a nevükben.³⁴ A tolvajok a legtöbb esetben ellopják néhányat a legfontosabb adataik közül (személyigazolvány szám, jogosítvány), majd az áldozat személyazonosságát felvéve hitelszámlákat nyitnak, az ezzel kapcsolatos leveleket pedig egy általuk megadott postacímre küldetik. A szükséges információkhoz könnyen hozzájuthatnak telefonon, illetve interneten keresztül, mivel sokan meggondolatlanul kiadnak személyes adatokat hiteligényléseken, illetve telefonos, internetes reklámokra válaszolva.³⁵ Előfordul, hogy egy internethasználó

³³ Vigyázz, ellophatják a személyazonosságod! <http://wol.jw.org/hu/wol/d/r17/lp-h/102001206> (2014.09.01)

³⁴ John Harrison személyiségét egy húsz éves fiatal Jerry Philips lopta el, aki 4 hónap alatt összesen 265 ezer dolláradósságot halmozott fel John nevében. <http://www.cbsnews.com/news/an-identity-theft-nightmare/>

³⁵ Az Internal Revenue Service minden költségvetési évben közzéteszi a személyazonosság lopással kapcsolatos bírói ügyeket. A 2014-es adatok a következő linken érhetők el: <http://www.irs.gov/uac/Examples-of-Identity-Theft-Schemes-Fiscal-Year-2014>

nem használja az adatvédelmi beállításokat a közösségi profiljain, könnyen megad személyes adatokat e-mailben, illetve nem lép ki az internetbankból ügyintézés után. Ezek a figyelmetlenségek mind veszélyforrásokká válhatnak. (Természetesen személyazonosság lopás az internet elterjedése előtt is létezett, azonban a felkészületlenség az internethasználatban könnyű prédává teheti az áldozatokat a tolvajok szemében.)

2.3 Az ismeret hiánya: Grooming

A „grooming” angol kifejezésre igazán pontos magyar definíció még nincs, legjobban a behálózás, becserkészés szóval írhatjuk körül a jelenséget.³⁶ A közösségi oldalak terjedésével leegyszerűsödtek az ismerkedés szabályai a felhasználók olyan emberek közeledését is elfogadják, akikkel még nem is találkoztak, de van közös ismerősük. Gyakran ez az „ismerős” egy fénykép mögött rejtőzve, magát 14 éves fiúnak mondó valaki a valóságban egy középkorú, vagy akár idős férfi, aki szexuális vágyai kiéléséhez keres áldozatokat a világhálón. Tudatosan felépített koncepcióval a közösségi hálókön vadászik fiatal fiúkra, lányokra. Ezek az elkövetők a fiatalok bizalmába férkőznek és a gyerekek sokáig észre sem veszik, hogy mi történik velük. A bizalmi viszonyt felhasználva személyes adatokat csálnak ki, interneten keresztül szexuális játékokba vonják be őket, legrosszabb esetben személyes találkozóra is sor kerülhet. A gyerekekben nagy izgalom és kíváncsiság, a szülőkkel ezekről a „barátokról” nem beszél, vagy szégyenérzete miatt általában nem, vagy túl későn kér csak segítséget.³⁷

2.4 Az ismeret hiánya: Depresszió, öngyilkosság

Az online média veszélyeire azok az öngyilkossági esetek hívják fel legjobban a figyelmet, amelyek esetében az internet az önagresszió oka. A Magyarországon is médianyilvánosságot kapó ügyben³⁸ egy fiatal lány, Amanda 2012-ben azért lett, 15 évesen öngyilkos, mert társai folyamatosan zaklatták, mind az online mind az offline világban. Egy róla készült meztelen fotó bejárta az internetet, zaklatója pedig akár iskolát váltott, akár más településre költözött, mindig a nyomában volt.

Hasonlóképpen internetes zaklatás áldozatává vált Hanna Smith³⁹, Ciara Pugsley, Erin Gallagher, nővére Shannon Gallagher, Jessica Laney, Anthony Stubbs, Joshua Unsworth,

³⁶ BARACSI (2012)

³⁷ NAIH „Kulcs a Net világához” p. 54

³⁸ Amanda Todd: <http://media-addict.hu/2012/10/17/amanda-todd-ongyilkos-lett-a-bantalmazott-lany/> (2014.05.02)

³⁹ Hanna Smith: <http://www.mirror.co.uk/news/uk-news/hannah-smith-suicide-teenager-used-2184385#ixzz3CiLxYj56> (2014.05.02)

Daniel Perry, Rebecca Sedwick⁴⁰ és a sort még folytathatnám. Egy Kanadai tanulmány szerint⁴¹ a közösségi oldalak használatának elterjedésével, mindinkább nő a cyber bulling-el (internetes zaklatás) összefüggésbe hozható öngyilkosságok száma. Az elkövetők főként tinédzserévek elején járó fiatalok, akiknek a személyisége még nem fejlődött ki teljes mértékben, és nagyon fontosnak tartják, hogy mit gondolnak róluk mások.

III. MIT TEHET A KÖZIGAZGATÁS A PRIVACY VÉDELEM TERÜLETÉN?

„Az államnak maximális felelőssége van az állami megfigyelések és adatbázisok területén. Ezen kívül meg kell szerveznie az oktatást és szabályozásról kell gondoskodnia.”⁴²

Az előző fejezetben említett megtörtént esetek bemutatják, hogy az állampolgárok sokszor nem tudják megvédeni önmagukat és jogaikat. Vajon ez azt jelenti, hogy a lakosságnak folyamatos rettegésben kell élnie, minden percben attól tartva, hogy valaki visszaél a személyes adataikkal, zaklatni fogja, kirabolja őket? A válasz természetesen nem. Az állampolgárok, s így az állampolgárok jogainak védelme az állam kötelezettsége.⁴³

Milyen feladatai vannak a közigazgatásnak az információs privacy védelem területén? Milyen szerepe van az oktatásnak, a civil szervezeteknek, a médiának? Mit tehetnek az egyének önmaguk védelme érdekében? A fejezet ezekre a kérdésekre ad választ.

3.1 Jogi és intézményi keretek

Privacy védelem 2011 előtt

A magyar jogi és politikai közvéleményben az adatvédelem az 1970-es évektől jelent meg, ugyanis ebben az időszakban került előtérbe „a gyengébb védelmének” elve.⁴⁴ 1978-ban a Polgári törvénykönyvben megsokasodtak a személyiségi jogokkal összefüggő rendelkezések, ekkor került be az a rendelkezés, amely kimondta, hogy a számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat.⁴⁵ A Ptk. 1992-es módosítása terjesztette ki a személyiségi jogok védelmét a számítógépes feldolgozás mellett, „a más

⁴⁰ Az internetes zaklatás áldozatai: <http://www.buzzfeed.com/ryanhatesthis/a-ninth-teenager-since-last-september-has-committed-suicide#1nteemu> (2014.08.04)

⁴¹ <http://www.cbc.ca/news/technology/cyberbullying-linked-suicides-rising-study-says-1.1213435> (2014.09.15)

⁴² ld. 31. lábjegyzet

⁴³ vö. Alaptörvény „Szabadság és Felelősség” I. cikk

⁴⁴ SÓLYOM (2005) pp.174-183

⁴⁵ 1977. évi IV. törvény; 1959 évi IV törvény (Ptk.) 83.§

módon történő adatfeldolgozásra”.⁴⁶ Az érintett tájékoztatási joga 1993-tól pedig általánossá és feltétel nélkülivé vált.⁴⁷

A Magyar Népköztársaság alkotmányának eredeti szövege a szabadságjogokat a „dolgozók” számára biztosította, az 1972-es alkotmánynovella pedig, miközben kiterjesztette a szabadságjogokat minden állampolgárra, előírta, hogy azokat a szocialista társadalom érdekeivel összhangban kell gyakorolni.⁴⁸ A személyiségi jogok, köztük az adatok védelme meglehetősen bizonytalan volt ebben az időszakban.

Kezdetben a személyes adatok védelmére vonatkozó törekvések az államnak és az adatfeldolgozónak való kiszolgáltatottság mérséklésére irányultak a hagyományos privacy-ideológiát tükrözve, melynek alapja a magánélet szentsége. A 80-as évek elejétől azonban az adatvédelmi szabályozási igény összekapcsolódott az állami működés átláthatósága iránti törekvésekkel. A német alkotmánybíróság híres népszámlálási ítélete adja a gondolat pontos megfogalmazását: „ha nem tudom, hogy mások mit tudnak rólam, akkor szabad döntésemben akadályozva vagyok”.⁴⁹

Döntő szerepet játszott a 80-as évek reformja, melynek következtében megtörtént az addig évente kétszer ülésező funkcióját veszített parlament valódi munkaparlamentté alakulása. A képviselők érdekeltté váltak abban, hogy megbízható és pontos információkhoz jussanak. Nagyon hamar követeléssé vált, hogy ne csupán a megbízhatósága alapján privilegizált sajtó, hanem minden egyes állampolgár megismerhesse a közérdekű adatokat, és tájékoztatást kapjon a róla nyilvántartott személyes adatokról.

Elkezdődött a nagy állami számítógépes nyilvántartások felépítése. Két nagy rendszer működött: az egyik az Államigazgatási Számítógépes Szolgálat, a másik pedig az Állami Népeség-nyilvántartó Hivatal volt. Ezek a szervezetek mindennemű jogi kötöttség, vagy cél nélkül bármely állampolgárról, bármilyen adatot gyűjthettek, „csak úgy” készletre, s ezeket az adatokat szabadon összekapcsolhatták. Az egyéneket felváltotta a személyi számok rendszere, s megvalósulni látszott az utópia mi szerint egy szám alapján mindent meg lehet mondani az adott személyről, az egészségügyi állapotától kezdve, az iskolai végzettségén keresztül, a

⁴⁶ 1992. évi LXIII. törvény 33.§

⁴⁷ 1993. évi XCII. törvény 40.§ (4) bekezdés a) pont

⁴⁸ 1949. évi XX törvény 54. § (2) bekezdés

⁴⁹ BVerfGE 65, 1. A szöveg elérhető a <http://www.servat.unibe.ch/dfr/bv065001.html> (2014.09.01) címen.

politikai-ideológiai nézetéig. Szerencsére a személyi számok rendszere a technika fejlődésének és a jogászok ellenkezésének köszönhetően hamar jelentőségét veszítette.⁵⁰

Ebben a kérdésben tökéletesen egyetértek David H. Flaherty megfogalmazásával, aki a következőket írta: „Sokak számára az egy számmal való azonosításnak dehumanizáló, önbecsülés-csökkentő hatása van. Hogy kik vagyunk, az különleges valami- legalábbis saját szemünkben az. Más szóval: identitásunk emberi méltóságunk része.”⁵¹

A KSH 1987-ben elkezdte az informatikai törvény előkészítését, azonban a rendszerváltás elsöpörte ezt a tervezetet. A Kerekasztal tárgyalások során külön (I/5. számú) albizottság állt fel „a tájékoztatás és az információ kérdései, az új tájékoztatási törvény” kidolgozására. A Magyar Köztársaság Alkotmányába⁵² bekerült az alapvető jogok közé a személyes adatok védelméhez és az közérdekű adatok megismeréséhez való jog.⁵³ Az Alkotmány rendelkezése alapján, sarkalatos törvény szabályozta a személyes adatok védelmének területét. Ez volt az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról, közismertebb nevén az Avtv.

Az Alkotmány a személyi és állampolgári jogok védelmére országgyűlési biztosokat nevezett ki (ombudsmani rendszer egy általános és három speciális biztossal). Ezzel összhangban az Avtv. nevesítette az adatvédelmi biztos intézményét (a személyes adatok védelme és a közérdekű adatok nyilvánossága érvényesülését alapjogvédő szemlélettel felügyelő országgyűlési biztos).

A biztoshoz bárki fordulhatott, ha véleménye szerint jogsérelem⁵⁴ érte, vagy annak közvetlen veszélye fennállt, kivéve, ha az adott ügyben bírósági eljárás volt folyamatban.⁵⁵ Azonban a törvény nem ruházta fel a biztost erős jogkörökkel. A privacy szabályozásának módosítására ajánlást, javaslatot nyújthatott be, jogsértés észlelése esetén pedig felszólítást tehetett a jogsértő adatkezelés megszüntetésére, ajánlásai azonban nem rendelkeztek jogi kötőerővel, felszólításainak figyelmen kívül hagyása pedig nem vont szankciót maga után.⁵⁶

⁵⁰Ld.: 2/1990. (II. 18) AB határozat, ABH 1990, 22, illetve 15/1995. (IV. 13) AB határozat, ABH 1991, 40.

⁵¹FLAHERTY (2001) p. 66

⁵²1989. évi XXXI. törvény az Alkotmány módosításáról

⁵³Magyar Köztársaság Alkotmánya 59. § (1)-(2) vö: JAKAB (2009) pp.2224-2240

⁵⁴KEREKES (2001) pp.121- 137.

⁵⁵Avtv. 27. § (1) bek.

⁵⁶Avtv.25. §

Privacy védelem 2011 után

A 2010-es kormányváltás követően a magyar jogi szabályozás az alkotmánymódosítással kezdve teljesen átalakult, az adatvédelmi szabályozás is új kereteket kapott.

Magyarország Alaptörvénye kiemelkedő helyen szabályozza az információs szabadságjogokat. Az állampolgári jogokat és kötelezettségeket felsoroló „Szabadság és Felelősség” elnevezésű fejezet VI. cikke a következőket tartalmazza:

„(1) Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák.

(2) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.

(3) A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel⁵⁷ létrehozott, független hatóság ellenőrzi.”⁵⁸

Az Alaptörvény szövegéből egyértelműen kirajzolódik a magánszféra védelem és a privacy védelme közötti szoros kapcsolat. Megfigyelhető, az információs szabadság jog új elemként megjelenik a személyes adatok védelme mellett. Korábban ezt a jogot az Alkotmány a véleménynyilvánítás szabadsága körében szabályozta. Kiemelkedő, hogy a törvényi szabályzás mellett egy új intézményt (Nemzeti Adatvédelmi és Információs szabadság Hatóság)⁵⁹ is létesít az Alaptörvény, melynek feladata az információs szabadságjogok érvényesülésének ellenőrzése.

Fontos megemlíteni, hogy a Büntető Törvénykönyv változásával,⁶⁰ a személyes adatokkal való visszaélés szabályozása is új formát nyert. A Btk. 219. §-a alapján két szintet különböztetünk meg: a bűncselekmény kategóriát, valamint a bűncselekmény szintjét el nem érő esetek kategóriája. Az előbbi esetben a Btk. rendelkezései, utóbbi esetben az Infotv rendelkezései irányadóak. Ezek alapján a büntetés a több milliós pénzbírságtól a 3 évig terjedő szabadságvesztésig terjedhet. Az új Polgári Törvénykönyv által bevezetett (a személyiségi jogok megsértése esetén fizetendő) sérelemdíj intézménye, pedig a személyiségi jogok védelmének további garanciáját szolgálja.⁶¹

⁵⁷ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban Infotv)

⁵⁸ vö.: ÁRVA (2013) pp.118-123

⁵⁹ a továbbiakban NAIH

⁶⁰ 2012. évi C. törvény A Büntető Törvénykönyvről (a továbbiakban: Btk.)

⁶¹ 2013. évi törvény a Polgári Törvénykönyvről. A lényegi rendelkezéseket a Ptk. 2: 46-48 § tartalmazza.

A közigazgatási privacy védelmi rendszer

Az Infotv alapfogalmakkal, alapelvekkel, adatvédelmi nyilvántartásokkal kapcsolatos rendelkezései az Avtv. szabályozásához képest szinte változatlanok. Miért volt szükség akkor az új szabályozás megalkotására? A törvény következetesebben ületi át a nemzeti jogba az EU Irányelveit, valamint szabályozza a NAIH működését.

„Tudomásul kell venni, hogy a jogi szabályozás arra jó, hogy előírja a sztenderdeket, illetőleg jogsértés esetén legyenek jogkövetkezmények. Az Infotv jobban szabályozza az adatbiztonság kérdését, mint a korábbi Avtv... az adatvédelmi hatóságnak van auditálási joga, ahol nem csak az adatvédelmi kérdéseket, hanem az adatbiztonsági követelményeknek a megvalósulását is figyelemmel követjük.”⁶²

A NAIH autonóm államigazgatási szerv, csak a törvényeknek alárendelten működik, feladatkörében⁶³ nem utasítható, függetlenségét biztosítja, hogy a Hatóságot vezető elnöknek politikailag is függetlennek kell lennie.⁶⁴ NAIH elnökének továbbá számtalan egyéb törvényi előírásnak kell megfelelnie.⁶⁵ A jogérvényesülés érdekében, ha a NAIH jogellenes magatartás észlel a felszólítást követően több, gyakorlati intézkedést tehet (akár 10.000.000 Ft-ig terjedő bírságot szabhat ki).⁶⁶

Az Alaptörvény és az Infotv. elfogadását megelőző időszakban újságírók és jogászok élesen bírálták⁶⁷ az ombudsmani rendszer megváltoztatására irányuló szándékot. Sokan úgy vélekednek, hogy az információs önrendelkezési jogok védelmét nem szabad egy hatóság felügyelete alá vonni, hiszen ez a megoldás csak elősegíti az emberi jogok figyelmen kívül

⁶² ld. 30. lábjegyzet

⁶³ Teljes körű felsorolásért lásd: Infotv. 38 §

⁶⁴ Infotv. V. és VI. fejezetek

⁶⁵ Infotv. 40 §

⁶⁶ Az eljárások részletes szabályozásáért lásd. Infotv VI. fejezetét.

⁶⁷ A kötelezettségszegési eljárás kiindulópontja: Magyarország megszegte a személyes adatok feldolgozása vonatkozásában az egyének védelméről és a személyes adatok szabad áramlásáról szóló 1955. 95/46/EK irányelvből fakadó kötelezettségeit, mivel idő előtt megszüntette az adatvédelmi biztos jogállását. Az irányelv előírja, hogy a rendelkezések érvényesülését független hatóság(ok) felügyelje(jék). Magyarországon ez a hatóság az Atv hatályba lépése előtt az adatvédelmi biztos volt, akit a szabályozás szerint az Ogy 6 évre választ. A 2008. szeptember 29-én kinevezett biztos Jóri András megbízatása, így 2014 szeptemberében járt volna le. Az Európai Unió Biztossága 2012. június 8-án az EK irányelv megsértése kapcsán keresetet nyújtott be az Európai Unió Bíróságához. Az ügyben (C288/12.) 2014. április 8-án hozott ítéletet a Bíróság. Az ítélet alapján „Magyarország **nem teljesítette** a személyes adatok feldolgozása [helyesen: kezelése] vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1955. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvből eredő **kötelezettségeit**.” Pervesztesként a Bíróság kötelezte Magyarországot a perköltség viselésére (kiemelés tőlem).

Az ítélet teljes szövege magyarul elérhető a <http://curia.europa.eu/> internetes oldalon.

hagyását. Természetesen mind a két fajta intézményrendszer mellett felsorakoztatható pro és kontra érvek sora.⁶⁸

Az ombudsmani rendszer „nagyon erős személyi, szervezeti és relatíve erős pénzügyi függetlenséget élvezett. A közigazgatásnak semmilyen lehetősége nem volt arra, hogy befolyásolja... a hivatali működés egyértelműen azt mutatta, hogy a hivatal betöltötte a szerepét.”⁶⁹

„Tudomásul kell venni, hogy az adatvédelmi hatóság egy teljes alkotmányos reform részeként jött létre. Ez egy olyan változtatás, ami kétségkívül kevesebb..., azonban az eltelt időszak alatt... nem tapasztaltuk ennek a negatív hatását. Az új bírságolási joggal [a hatóság] hatékonyabban fel tud lépni...⁷⁰ Biztos, hogy jobb ez a konstrukció.”⁷¹

3.2 Közoktatás

Ahogy a második fejezetben utaltam rá az internethasználók gyakran minden körülmények nélkül, önként veszélyeknek teszik ki magukat, ennek oka pedig az ismerethiány. Miért állítom ezt, amikor a jogszabályok nyilvánosak, a különböző közigazgatási intézmények működése megismerhető, a közösségi oldalak, mobiltelefon alkalmazások privacy policy-ja szintén nyilvános, sőt a felhasználóknak kötelességük lenne elolvasni és értelmezni ezeket a szabályzatokat? Személyes tapasztalatom, kutatási eredményeim, illetve az alábbi két idézet is alátámasztja ezt a gondolatot:

„... bár a jogi rendelkezésekkel az emberek nagyjából tisztában vannak... de azzal, hogy ők mit tehetnek nem. Az adatbiztonsági beállítások, programok területén hiányosak az ismeretek. Itt a képzés, kampányok, reklámok, felhívások kifejezetten hasznosak lehetnek... a fiatalok nem tudnak kihez fordulni, szinte csak egymás között beszélnek meg a felmerülő gondokat... a probléma orvoslásában az oktatásnak jelentős szerepe lehet.”⁷²

„Már a legkisebb gyerekek is [tudatosan] nyomkodják a szüleik telefonját, sok házi feladat elkészítése az általános iskolákban már számítógépen történik. Szerintem mindenképpen foglalkozni kell az adatvédelemmel, akár az általános iskola elejétől a számítástechnika óra keretében, de nem tartok elképzelhetetlennek egy külön foglalkozást az internetes viselkedés oktatására. Ezen kívül az állampolgári ismeretek, valamint a médiaismeret órák során lehetne

⁶⁸ A NAIH közleményei, határozatai, állásfoglalásai, az adatvédelmi nyilvántartással és audittal kapcsolatok információk, valamint az Adatvédelmi Biztos Irodájának Archívuma a <https://www.naih.hu> oldalon érhetőek el.

⁶⁹ ld. 3. lábjegyzet

⁷⁰ vö. JÓRI (2010) p.56

⁷¹ ld. 30. lábjegyzet

⁷² ld. 30. lábjegyzet

az információs önrendelkezési jogról tanulni, illetve fogyasztóvédelmi kérdésekre is ki lehet térni”⁷³

A Nemzeti Alaptanterv⁷⁴ célul tűzi ki a médiatudatosságra való nevelést, hogy a tanulók „értsék a média nyelvét, megismerkedjenek a média és a társadalom közötti kölcsönös kapcsolatokkal, valamint a kérdés jogi és etikai jelentőségével.”

Áttanulmányoztam a NAT médiaismeret, informatika, etika/erkölcstan, társadalmi, állampolgári és gazdasági ismeretek tárgyakból, megállapításom szerint ezek a tantárgyak adhatnák az iskolai oktatásban az adatvédelmi ismeretek alapját. Az informatika a fizikai háttérrel, az alkalmazások használatának fortélyait tanítja meg, a média a figyelmet ezeknek jogi szabályozására irányítja. A társadalmi, állampolgári és gazdasági ismeretek az információs társadalom működésével és magukkal az állampolgári jogokkal foglalkozik, az etika pedig hozzá segíti a tanulókat, hogy napjaink globalizálódó világában meg tudják őrizni személyiségük integritását, elegendő önismeretük legyen, hogy felismerjék és elkerüljék az online lét veszélyeit. Láttam hasonló törekvéseket a NAT-ban, azonban ezekre a témákra véleményem szerint túlkésőn, először csupán az 5-6. osztályban kerül sor (A megállapítás alól kivételt képez az informatika tárgy, az 1-4. évfolyamokon a diákok megismerkednek a netikett szabályaival és a személyes adatok fogalmával).

Teljes mértékben egyetértek Hidvégi Fanny véleményével: „Muszáj megértetni velük, hogy milyen információval és hogyan lehet visszaélni. Meg kell tanítani a biztonsági és adatvédelmi beállítások lényegét, illetve meg kell említeni, hogy bizalmas adatokat ne adjon meg senkinek... Nem kell és nem is lehet megtiltani [a közösségi oldalak] használatát, mert... az iskolában a gyermek padtársa úgyis megmutatja, hogy kell belépni. Ha [az Internetet] szülő tudtán kívül használja a gyermek, annak nagy veszélye van”

Meglátásom szerint a pedagógusoknak a jelenleginél sokkal nagyobb figyelmet kellene szentelniük az e-privacy védelem oktatásának, így azok a gyermekek, akik most kerülnek be a közoktatásba tudatosabb internet használókká válnak. Célszerű lenne a NAIH által kiadott „Kulcs a Net világához” című tanulmány ismeretét és használatát. A tanulmány fő része a pedagógusok számára nyújtana információs bázist a problémákkal és a jó gyakorlatokkal kapcsolatban, a függelék anyaga pedig sikeresen felhasználható lenne az oktatás során, mivel

⁷³ ld. 31. lábjegyzet

⁷⁴ a továbbiakban NAT. Magyar közlöny 2012. évi 66. szám, pdf formátumban letölthető:
<http://www.magyarokozlony.hu/dokumentumok/14d304dac9b0a08bf05894888b6ea3a2d1846e4e/megtekintes>
(2014.09.15)

a gyermekeknek szóló információk és feladatok egyszerű nyelvezettel vannak megfogalmazva, sok a színes illusztráció és a figyelemfelkeltő feladat.

Hogyan valósulhat meg az ügyfélképzés azoknak az állampolgároknak az esetében, akik már kiestek a közoktatásból? Úgy vélem a társadalmi célú hirdetések és egyéb kampányok, valamint a civil szervezetek közreműködésén keresztül. A továbbiakban ezeket a területeket fejtem ki.

3.3 Kampányok, civil szervezetek és privacy szakértők

A privacy védelem nem valósítható meg csupán az állam közreműködésével, sokkal inkább a jogalkotóknak, közigazgatási szerveknek, a civil szervezeteknek, a privacy szakértőknek, az újságíróknak és az egyéneknek együttesen kell egy társadalmi szövődéket, egy privacy védő hálót alkotniuk. Így azokhoz az állampolgárokhoz, akik már kiestek a közoktatásból, eljut az e-privacy ügyfélképzés.

A TASZ civil szervezet célkitűzése, hogy felvállalja a mediátor szerepet. „Szeretnénk létrehozni ismeretterjesztő blogot, illetve egy csapatot, akik praktikus szolgáltatásokat, megoldásokat nyújtanak, népszerűsítsenek jó megoldásokat. Például a Tor software-t.”⁷⁵ Jelenleg készül egy videójuk a Józsefvárosi arcfelismerő rendszerekkel kapcsolatban. A NAIH szintén részt vesz országos kampányokban, a Safer Internet Day⁷⁶ rendezvényein, valamint nemrégiben készült el Vastag Tamással közreműködésével, a „Kell egy biztos hely” című ingyenesen letölthető videóklipp.

Úgy gondolom, szükség lenne arra, hogy az e-privacy-val kapcsolatos visszaélések nagyobb médianyilvánosságot kapjanak, jelenjen meg rendszeresen az online médiával foglalkozó magazin (példaként említem az Amerikai „Wired” magazint), valamint legyenek megkapó társadalmi célú hirdetések, melyek egyaránt szólnak a felnőtteknek és a fiataloknak.⁷⁷

Több nemzetközi példa is felhozható sikeres privacy kampányokra. A Cseh Adatvédelmi Szolgálat rendszeresen megszervezi a „My privacy. No peeking, no poking” elnevezésű versenyét, melynek célja a privacy tudatosság erősítése a gyerekek körében,⁷⁸ és a Iuridicum Remedium nevű NGO minden évben közzéteszi a „Big Brother Awards” listát, amely a legrosszabb, tevékenységük során magánéletet sértő hatóságok, vállalatok jegyzékét tartalmazza. A lengyel Panoptykon Foundation e-privacy védelemmel foglalkozó civil

⁷⁵ ld. 31. lábjegyzet

⁷⁶ Az EU finanszírozású Safer Internet Program honlapja: <http://www.saferinternet.org/>

⁷⁷ Jelenleg Magyarországon a Médiaunió „Neked 8?” című kampánya folyik (<http://neked8.mediaunio.hu/>)

⁷⁸ A kampányról részletesebben: <http://www.uoou.cz/pro-mladez/ds-2331/p1=2331> (2014.09.01)

szervezet, oktatási programjuk, média megnyilvánulásai világszerte ismertek.⁷⁹ Az USA-ban ebben az évben a kampányoknak köszönhetően 20-nál több tagállam alkotott új „student privacy” törvényt (pl.: „Do NOT Call”, „Do NOT Track”, „Data Quality Campaign”). Az iKeepSafe nemzetközi non-profit szervezet erőforrásokat és szolgáltatásokat biztosít kifejezetten iskolák részére.⁸⁰

3.4 Az egyén felelőssége

„Nagyon fontos... annak a tudatosítása, hogy nincs adatvédelem adatbiztonság nélkül. A kettő csak együtt létezik. Bármilyen jogi szabályok is vannak, ha nincs meg a megfelelő biztonság. Ebben a vonatkozásban nem csak a szolgáltatóknak, nem csak a honlapok üzemeltetőjének van kulcsszerepe, hanem magának a felhasználónak, főleg a személyes beállításokkal.”⁸¹

Hiábavalóak a jogszabályok és az ügyfélképzés, ha a felhasználók nem tartják fontosnak az e-privacy kérdését. „Fel kell hagyni azzal az ostoba gondolkodásmóddal, hogy akinek nincs titkolnivalója, annak nem érdekes, hogy milyen adatait szerezhetik meg. Az élet legszemélyesebb részről szólnak az online térben létező adataink...”⁸² Minden egyes embernek el kell gondolkoznia azon, mennyire tartja fontosnak a jogait. Az egyéni felelősség hiányában az e-privacy halott ügy.

KÖVETKEZTETÉSEK

Összefoglalásul fontosnak tartom megállapítani, hogy az e-privacy kulcsfontosságú, „hot topic” kérdés. Ahhoz, hogy az állampolgárok teljes körű védelme megvalósuljon, széleskörű (nemzetközi) összefogásra van szükség. Elsősorban célszerű lenne megvalósítani egy oktatási reformot az e-privacy területén, valamint úgy vélem hasznos lenne, a közoktatásból már kiesett állampolgárok számára egy ingyenes privacy védelmi oktatás megszervezése. Továbbá, célszerű lenne a hazai privacy védelmi kampányok kibővítése a NAIH és a civil szervezetek összefogása által, online és offline kampánycsomag keretében.

Gyakran maguk a szakértők sem tudják pontosan, hogy milyen módon váltja ki egy kampány a hatását. Nagyon nehéz lemérni az emberi gondolkodásmód változtatását, azonban a cél: lépéseket tenni, hogy a privacy védelem a mindennapok része legyen, a személyes adat pedig valódi értéké váljon minden egyén szemében. Ennek eléréséhez szükségesnek tartom, hogy

⁷⁹ Panoptikon Foundation hivatalos honlapja: <http://panoptikon.org/>

⁸⁰ http://www.ikeepsafe.org/educators_old/digital-compliance-and-student-privacy-a-roadmap-for-schools/ (2014.09.01)

⁸¹ ld. 30. lábjegyzet

⁸² ld. 31. lábjegyzet

minden egyes állampolgár ismerje és értékelje az alapvető emberi és állampolgári jogait. Ahhoz, hogy az állam- állampolgár kapcsolat jól működjön, az állam vezetésének fel kell ismernie, hogy a digitális korban a polgárok védelme egyre összetettebb és fontosabb feladat. E felismerés segíthetne, hogy a problémák gyökerét találják meg, ne csak a tüneteit kezeljék.

MELLÉKLETEK

INTERJÚK

Dr. Majtényi László

Hogy látja, a magyar állampolgárok mennyire vannak tisztában a jogaikkal?

A magyarok kifejezetten önérzeteseek, a jogaikra kényesen büszkék. A kommunizmus után a privacy érzékenység rendkívül erős volt, az állampolgárok határozottan léptek fel a totalitárius állam visszaéléseivel szemben.

Milyen általában véve az állampolgárok digitális írástudása?

Fontos, hogy nem csak abban kell különbséget tennünk, hogy valaki digitálisan analfabéta-e vagy sem, hanem a digitális írástudásnak több szintjét is meg kell különböztetnünk. Véleményem szerint a digitális analfabetizmus jelentősen visszaesett az évek során, de ez nem azt jelenti, hogy aki el tud küldeni egy elektronikus levelet, vagy használ egy közösségi hálót, az képes közigazgatási ügyintézésre is. Az emberek többsége az önkormányzati ügyintézésen inkább szeretne minél gyorsabban túlesni, én magam is inkább bemegyek a hivatalba, minthogy ügyeimet az interneten keresztül intézzem el, gondolják helytelenül.

A 80-as évek óta sokat változott előnyére a közigazgatás, azonban a fejlődés még nem elég. Ideális esetben a közigazgatást ügyfélbarátság jellemzi és olyan egyszerű a digitális ügyintézés, mint egy e-mail megírása, sőt, ha kell az ügyfél akár telefonos ügyfélszolgálatos segítséget is kaphat, ma azonban ettől még távolabb állunk. A mostani használathoz a polgároknak magas szintű felkészültség kell.

Miért tartja fontosnak, hogy az emberek figyelmet fordítsanak a személyes adataik védelmére?

Nekem ez a kérdés évtizedek óta a szívügyem. Az emberek szempontjából pedig kifejezetten fontosnak tartom. Az egyszerű válasz: annyiban vagyunk szabad emberek, amennyiben magánéletünk lehet. Tehát ha a magánéletünket elveszítjük, a szabadságunkat is elveszítjük. Ezért kell az állam és a piac adatéhségével szemben gátakat emelni. Ez a funkciója a személyes adatok védelmének. Egy független ellenőrző szervezetre is szükség van, mivel olyan típusú jogsértésekkel állunk szemben, amelyek egy-egy ember ingerküszöbét nem feltétlenül haladják meg (pl 1 direktmarketing) tömegében azonban a pici jogsértések, nagy jogsértéssé állnak össze. Erre több nemzetközi példa van.

Összefoglalva: amennyi információt valaki tud rólam (természetesen olyan információk, amelyeket magam részéről szeretnék eltitkolni) annyiban a hatalmában vagyok. Ha most Önről a gyerekkori csínytevésektől, a mai magánéleti titkaiig mindent tudnék, olyan dolgokat, amiket maga nem szívesen kötne az orromra, akkor én ezzel hatalmat gyakorolhatnék Ön felett és ezt kellene elkerülni.

Mit gondol, az államnak miért kell figyelmet fordítani arra, hogy az emberek tudjanak erről a kérdésről? Érdeke az államnak, hogy az állampolgárok személyesen tájékozottak legyenek az információs önrendelkezési jogaikról?

Ez egy nagyon érdekes intellektuális és társadalmi „csapda” tudniillik az államnak nem érdeke, az államnak az az érdeke, hogy minél többet tudjon. Azt kell mondanom, hogy ez egy sok ezer éves dilemma. Az öntözéses kultúráktól, az istenkirályoktól egészen napjainkig az államnak alapvető természetes igénye, törekvése, hogy minél többet tudjon az állampolgáiról. Egyrészt ezt hatékonysági szempontból, de mindenekelőtt hatalmi szempontból lehet indokolni.

A kérdés az, hogy tekinthető-e a személyes adatok védelme protektív jognak, természetesen nem, hanem úgynevezett önrendelkezési jog, az államnak „el kell viselnie” az polgárainak önrendelkezési jogát. Azt tudni kell, hogy minden állam tekintet nélkül- még a liberális állam is, ami elvben ezeket tiszteletben tartja- abszolút érdekelt abban, hogy ezeket a jogokat megsértse. Rengeteg példa van arra, hogy az USA-ban, mely mintapéldája lenne a liberalizmusnak, milyen durván sértik meg a polgárok az információs önrendelkezési jogát.

Ha az államnak nem érdeke az állampolgárok tájékoztatása, akkor hogyan ítéltük meg az adatvédelem témáját célzó társadalmi célú hirdetéseket, kampányokat? Folyamatosan működik az EU támogatású „safer internet” honlap, valamint a legújabb „Neked 8?” kampány.

Az állam mindig a piac visszaéléseire szereti felhívni a polgárok figyelmét. Erre meg mondhatom, hogy most készül egy jogszabálytervezet a közterületen elhelyezett arcfelismerő rendszerek, illetőleg a közlekedési célból működtetett közlekedést ellenőrző információs rendszerekről. Ezeket kívánják korszerűsíteni, illetve más adatbázisokkal összekapcsolni. Tehát az állam, szerintem most különösen „cinkelt kártyákkal” játszik.

Az államnak alapvető feladata, hogy a legitimációját folyamatosan erősítse, hiszen a létezésének legfontosabb eleme a társadalmi elfogadottság. Az állam mindig fellép civilizatórikus keretben, de ezekben az információs ügyekben - ezek mellett a hangzatos

kezdeményezések mellett, amelyeket említett-, a társadalom mind teljesebb ellenőrzése iránti törekvéseket kell látni.

Az alkotmányosságot sérti, hogy a TEK bírói ellenőrzés nélkül jogosult az én lehallgatásomra. Arra gondolok, hogy a mi beszélgetésünket a TEK rögzíti-e, mi sohasem fogjuk megtudni. Tekintettel arra, hogy nincs bírói kontroll, ami nyilvánvalóan alkotmányos követelmény és a rendőrségi törvény is így szabályozza a bűnüldözési célú megfigyeléseket, ez az alkotmányos elemi jogokat sérti.

Ezért, ha nekem Ön az államot dicséri, akkor rossz ajtón kopogtat be. Éppen az elmúlt 1-2 évben nagyon durva dolgok történtek a magánélet védelme terén az állam túl hatalma növelése érdekében, és ez nyilvánvalóan alkotmányellenes. Itt olyan dolgok történnek, amiről azok, akik ezeket, megfogalmazzák, tökéletesen tisztában vannak, hogy a Strassbourg-i emberi jogi bíróság joggyakorlatával és az európai szabadelvű alkotmányos kötelezettségekkel teljes mértékben ellentétesek. Ezek alapján az állam jóindulatát ebben a kérdésben egyáltalán nem tudom visszaigazolni.

Ezek alapján, ha az állam nem tudja elvállalni ezt a szerepet, akkor kinek a felelőssége az emberek tájékoztatása? Az oktatásnak, a civil szervezeteknek?

Látni kell, hogy van állami feladat: az államnak tiszteletben tartania a független intézményeket. A társadalomnak nyilvánvalóan feladata lenne, de ezt a feladatot biztosan nem fogja ellátni, hogy a független adatvédelmi intézményrendszer helyreállítását követelje. (Ami ugyancsak megszűnt az állam jótékonyága következtében.) Az ombudsmani jogvédelmet nyilvánvalóan helyre kellene állítani.

Másrészt vannak civil törekvések, pl: TASZ szervezetnek van magánélet védelmi programja, jogsérelmet szenvedett állampolgárok érdekvédelmét is ellátja. Hasonló tevékenységet folytat a Helsinki bizottság, valamint az Eötvös Károly Közpolitikai Intézet is, ha nem is individuális jogvédelem, de például a TEK alkotmányosértő hatáskörét az Alkotmánybíróságon megtámadtuk. Az Alkotmánybíróság, ami ugyancsak politikai befolyás alatt áll pillanatnyilag, egy nem lényegtelen elemben érveinket elfogadta. Nevezetesen azt, hogy ha miniszter engedélyezi a magánszemély teljes, gyakorlatilag korlátlan ellenőrzését, akkor a Nemzetbiztonsági szolgálatoknak és a Terrorelhárítási Központnak az állampolgárok telefonjának, elektronikus levelezésének, a testi megfigyelésének, a videó megfigyelésének, a hálózobájának lehallgatására mindenre joga van egy miniszteri aláírás által, tulajdonképpen jogi érvelés, indoklás nélkül. Fel sincsenek sorolva azok a tényállások, amelyek esetén a

megfigyelés elrendelhető. Legalább legyen indoklás, mondta az AB! Ezzel szemben a rendőrségi törvényben meghatározott gyanú esetén bírói felülvizsgálathoz van kötve a megfigyelés lehetősége. Az Alkotmánybíróság annyit megtett, hogy a megfigyelés elrendelését indokolni kell, az ügy pedig most Strassbourghban van.

A civil kezdeményezések mellett pedig meg van a feladatuk az újságíróknak, a felsőoktatásban résztvevőknek, akik szabadságjogokat tanulnak és az adatvédelmi szakértőknek. Ennek együttesen kell egy szövődéket, egy a társadalom védelmét szolgáló hálót képeznie. A kaukázusi országokban az újságírókat néha lelövik az utcán a munkájuk miatt, de Magyarországon ilyen nem történik meg. Miért nem történik meg nálunk? Mert eltér az államkultúra és az állampolgárok kultúrája, a magyar társadalom ezt nem tűri. Ugyanez van az információs jogok területén is a diktatúrák teljesen korlátlanul ellenőrzik az állampolgárokat (a digitális korban ez különösen veszélyes).

Egyébként nagyon fontos az egyéni szint is, az hogy valaki privacy-barát technológiákat használ, saját online működésénél bizonyos óvintézkedéseket tesz közösségi oldalakon. Ezek egyéni dolgok, amik összeadódnak társadalmi szintre.

Az egyéni szintnél maradva, Ön szerint mik lehetnek azok az alapvető ismeretek, amiket minden állampolgárnak tudnia kellene?

Alap dolog az, hogy amikor az ember internetezik akkor egy ilyen „hosszú vörös csíkot” hagy maga után. Tudni kell, hogy bizonyos felületeken a magánélet mennyire korlátozott. A társadalmat nevelni kell! A társadalom nevelését pedig egyrészt képzett szakértőknek kell ellátnia, másrészt ezt feladatuknak tekintő társadalmi szervezeteknek és ezen túl nyilvánvalóan meg van az állami kötelezettség is, de ezt mindig megfelelő gyanakvással kell tekinteni

Ha az Infotv-t nézzük: milyen szintű védelmet nyújt a magyar állampolgároknak az Unió tagállamokhoz viszonyítva?

Az Infotv-ben a legjobban látható szövegszerű visszaesés az információs szabadság terén van, a személyes adatok védelme vonatkozásában szabályai ma is kiállják az európai sztenderdeket. Hibák vannak benne, sokkal inkább hibák (dogmatikai is), mint jogkorlátozások.

A legfőbb probléma a védelmi rendszernek a meggyengülése. Közigazgatási intézménnyé alakították át a független ombudsmani szervezetet, és nagyon érdekes meg lehet nézni a NAIH már több mint 2 éves fennállása óta soha az államrezont érintő kérdésben nem védte meg a magyar állampolgárokat. Tehát „izmozik” banokkal, kftkkel és (ezt egy kollegám

megnézte) független vagy ellenzéki irányítású önkormányzatokkal. Nyilvánvaló a politikai befolyásoltság, és azt is megtette a politikai marketing tekintetében, hogy a hivatal vezetője a jogkorlátozás mellett lépett.

Mi volt az előnye az ombudsmani adatvédelmi rendszernek?

Nagyon erős személyi, szervezeti és relatíve erős pénzügyi függetlenséget élvezett. A közigazgatásnak semmilyen lehetősége nem volt arra, hogy befolyásolja. Persze nagyon sok múlik a személyeken is, nyilván politikai befolyásolásra akadhatnak példák, de a hivatali működés egyértelműen azt mutatta, hogy a hivatal betöltötte a szerepét.

Úgy gondolom, hogy elég primitív az a gondolkodás, amely azt mondja, hogy nincsenek független hivatalok, mert mindent emberek csinálnak. Az igazságnak egy morzsája valóban itt van, de ahol garanciák tömegével védik egy hivatal függetlenségét, és a személyt nem politikai kegyből helyezik oda, hanem egy meritokrata jelölés alapján ott beszélhetünk valódi függetlenségről. Ez a civilizált világban egy teljesen bevett dolog. Pl: nem lehet valaki az USA legfelsőbb bíróságának elnöke, csak mert valamelyik politikus pártfogását élvezzi, ez teljesen egyértelmű. Tehát léteznek független intézményrendszerek, de ez ma Magyarországon megszűnt.

Akkor a megoldás ezek szerint az lenne, ha visszaállítanák a független adatvédelmi biztosi rendszert?

Igen! Ha az alkotmányosságot Magyarországon helyreállítják, akkor vissza is kell állítani az ombudsmani rendszert. Bár erős a gyanúm, hogy nem fogják ezt visszaállítani. Legalábbis nem a megfelelő szinten.

Látnunk kell, hogy Magyarország 1992-től egy alkotmányos mintaállam volt. Az adatvédelem tekintetében ide jöttek tanulni a Nyugat-Európai döntéshozók, a magyar szisztémát vette át sok Nyugat-Európai ország. Szent István óta erre nem volt példa a magyar közjogban és most ezt rombolták le.

Amikor a magyar jogállamot egyszer helyreállítják, nekem erőteljes gyanúm, hogy igencsak fékezett jogállami állapotot hoznak létre, ami a mostani, és az alkotmányos mintaállam között áll majd, és nem fog visszatérni a jogállami feladatok gyökeréhez, amit egyébként meglehetősen fájdalmasnak tartok. Azt gondolom, hogy annyira kilengett az inga egy autoriter irányba, hogy már soha nem fog visszamenni oda, amit 90-ben kitaláltak. Nagyon érdekes a dolog, hogy 90-ben volt egy alkotmányos mintaállam, amit egy végtelenül züllött

politikai elit működtetett, ami magát az alkotmányos szerkezetet is diszkreditálta a magyar társadalom szemében.

Budapest, 2014.07.08

Dr. Péterfalvi Attila

Hogy látja, a magyar állampolgárok mennyire vannak tisztában a jogaikkal?

A magyar emberek ismerik a jogaikat, ezt támasztja alá, hogy az adatvédelem területén, a panaszbeadványok száma folyamatosan növekszik. Legtöbb esetben az állampolgárok akkor is hozzánk fordulnak, ha vélt jogsérelem van, tehát csak a gyanú áll fenn.

Az információs önrendelkezési jogok területén milyen problémákkal találkozhatunk?

Probléma legtöbbször a marketing jellegű adatkezelésekkel van pl. bankok, pénzüzetek esetén. Az állampolgárok kényszerhelyzetben vannak, vagy a nyilatkozatok nem egyértelműek és világosak. Fontos szabály, hogy nem lehetnek megtévesztő módon elrejtve olyan utalások, amelyek teret engednének a visszaéléseknek, ez igaz akár egy egyszerű nyilatkozat, akár a jogszabályok esetén is.

Állami adatkezelések, mindig jogszabályon alapuló kötelező feladatok, melyek esetén az állampolgár, mint ügyfél jogai részletesen meghatározottak, ám hibák előfordulhatnak. Negatív példa lehet a 2006-os kormányrendelet a gázár támogatásról. A polgároknak kérelmet kellett benyújtaniuk a jegyzőhöz (részletes jövedelemigazolás, vagyoni helyzet felmérése), amit a jegyző az APEH-en keresztül ellenőrzött vissza. Azonban a rendeletben nem volt arra vonatkozó feljegyzés, hogy ezeket az adatokat, hol, meddig és milyen formában tárolják majd. Felhívással éltem a kormány felé, a kormány indoklása az volt, hogy az adatközlés önkéntes alapon történt. Ez egy érdekes kérdés, úgy látom, hogy az a személy, aki gázár támogatást igényel nincs választási helyzetben, mert el kell döntenie, hogy a pénzéből kenyeret vegyen, vagy befizesse a fűtésszámlát. Fontos ezért odafigyelni arra, hogy ami önkéntes az nem feltétlenül tisztességes. Később a szabályozást kiegészítették az adatkezelésre vonatkozó részekkel.

Az állampolgárok részéről valós veszélyt jelent a közösségi portálok és az internet használata, ahol legtöbbször úgy adnak az felhasználók hozzájárulást, hogy nem olvassák el a privacy policy-t. Másrészt az állampolgároknak nagyon nehéz megérteni a közérdekű adatok, közérdekből nyilvános adatok stb. bonyolult rendszerét.

Ön szerint ma Magyarországon milyen az embereknek a digitális írástudása? Milyen hiányosságokkal találkozik, és milyen megoldás lehetne ezekre a nehézségekre?

A legnagyobb hiányosság a közösségi oldalakkal kapcsolatban látható. Nem véletlenül kezdtünk bele gyerekjogi projektünkbe, aminek elsődleges célja a figyelemfelhívás. A közösségi oldalak vizsgálatának több aspektusa van, csak az egyik az adatvédelem, többek között szociológiai és egyéb megközelítésben is fontos kérdés. Úgy látom, hogy bár a jogi rendelkezésekkel az emberek nagyjából tisztában vannak, de azzal, hogy ők mit tehetnek nem. Tehát az adatbiztonsági beállítások, programok területén hiányosak az ismeretek. Itt a kampányok, reklámok, felhívások kifejezetten hasznosak lehetnek.

Külön probléma, hogy a fiatalok nem tudnak kihez fordulni, szinte csak egymás között beszélnek meg a felmerülő problémákat, mert nyilván a szülő nem ért hozzá, a pedagógus pedig egyrészt a pozíciója miatt, másrészt pedig az életkora miatt elérhetetlennek tűnik. Úgy gondolom, hogy a probléma megoldásában az oktatásnak jelentős szerepe lehet. Ennél fogva ajánlottuk a miniszter figyelmébe a kiadványunkat, mely beépülhetne a Nemzeti Alaptantervbe. A *Kulcs a Net Világához* kiadvány célja, hogy adjon egy problématérképet, szerepeljen benne az, hogy hova lehet fordulni, ha jogsérelem merül fel, és az is, hogy a segédanyagokkal (internetes napló, kérdőív) mindenki le tudja mérni mennyire tudatos internethasználó. Szeretnénk, ha a fiatalok átgondolnák, hogy milyen fizikai, érzelmi következményeik lehetnek azoknak az tetteknek (például bullying), amelyeket ők egyszerű diákcsínyekként kezelnek.

Mennyire használja ki a közigazgatás az internet adta lehetőségeket?

Az biztos, hogy ma Magyarországon az internetnek a közügyek intézésére történő használata, még mindig közel sem olyan arányú, mint amilyennek lenni kellene, vagy amilyen lehetne. Gyakorlatilag az elektronikus aláírás szinte nem működik, az ügyfélkapuval kapcsolatban pedig általában van egy bizalmatlanság az ügyfelek oldaláról, másrészt pedig ezeknek az elterjedése sem olyan mértékű, mint ami kívánatos lenne. Ez lehet pénzügyi kérdés, közigazgatási kérdés és bizalom kérdése is.

Ha az adatvédelem területére gondolunk, milyen közigazgatási megoldásokat lát hatékonnak, figyelemfelkeltőnek?

Készül majd reményeim szerint egy rövid társadalmi célú hirdetés a Vastag Tamással elkészített „Kell egy biztos hely” című ingyenesen letölthető videóklipp alapján. Jelenleg részt veszünk lengyel vezetéssel gyermekjogi projektbe, melyre most nyertünk EU-s

pályázatot. Úgy gondolom, az adatvédelemre fel lehet, sőt fel kell hívni a figyelmet, de ez főként a közösségi portálokkal kapcsolatban érvényesülhet.

Mit mondhatunk a folyamatosan működő safer internet honlapról, vagy a most indult „Neked 8?” kampányról? Mennyire képesek elérni a céljukat?

Ezek a kampányok nagyon hasznosak. E mellett rendkívül figyelemfelkeltő az International Safer Internet Day. Ezen a napon olyan rendezvényeket és kampányokat szerveznek hazai és nemzetközi téren, amelyek középpontjában az adatvédelem áll. Kifejezetten üdvözlöm az ingyenes letölthető szűrőprogramokat is.

Jogi szemszögből nézve, mit fontos kiemelni az adatvédelem témakörében?

Ami nagyon fontos – és ebben a vonatkozásban az új adatvédelmi szabályozás igen pozitív- annak a tudatosítása, hogy nincs adatvédelem adatbiztonság nélkül. A kettő csak együtt létezik. Bármilyen jogi szabályok lehetnek, ha nincs meg a megfelelő biztonság. Ebben a vonatkozásban nem csak a szolgáltatóknak, honlapok üzemeltetőjének van kulcsszerepe, hanem a felhasználónak, főleg a személyes beállításokkal.

Tudomásul kell venni, hogy a jogi szabályozás az arra jó, hogy előírja a sztenderdeket, illetőleg jogsértés esetén legyenek jogkövetkezmények. Az adatbiztonság azért fontos mert azzal sok minden megakadályozható. Az új Infotv jobban szabályozza az adatbiztonság kérdését, mint a korábbi Avtv. Illetve az adatvédelmi hatóságnak van auditálási joga, ahol mi is nem csak az adatvédelmi kérdéseket, hanem az adatbiztonsági követelményeknek a megvalósulását is figyelemmel követjük. Nyilván ez nem olyan mélységben valósul meg, mint amit a nemzetvédelmi felügyelet lát el.

Az Európai Bíróság keresőmotorokkal kapcsolatos ítéletének fontos az adatvédelmi aspektusa. Mit kell erről tudni?

A probléma alapvetően az a filozófiai különbözőség, ami az európai adatvédelem és az USA privacy felfogás között áll. Ez igaz a keresőmotorokkal kapcsolatban is. Jelenleg egyeztetés alatt áll, hogy hogyan, vagy milyen kérdésekre vonatkozóan lehet az európai hatóságoknak egységesen fellépni. Mivel, ha európai polgárok adatainak a kezeléséről van szó, akkor függetlenül attól, hogy a szerverek hol vannak a világon, arra az EU szabályait kell alkalmazni. Természetesen a nagy cégeknek, így a Google-nak is más elképzelésük van erről a kérdésről.

Az Infotv mennyiben felel meg az európai sztenderdeknek? Szükséges esetleg változtatásokat tenni?

Az EU sztenderdeknek ételemszerűen megfelel, azonban az ténykérdés, hogy vannak politikai motivációkból eredő olyan vélemények, miszerint az előző szabályozás és az előző konstrukció volt. Én ezeket a véleményeket nem osztom. Fontos rögzíteni, hogy a magyar adatvédelmi szabályozással szemben jelentek meg kritikák, de ezek a kritikák főként az átalakítás módjára vonatkoztak, arra, hogy a korábbi adatvédelmi biztos miért nem töltötte ki a mandátumát, nem magára az érdemi adatvédelmi szabályokra.

A jelenlegi konstrukció szerint is az adatvédelmi hatóság teljesen független, a pénzügyi függetlenségét mintaértékűnek tekintik azáltal, hogy a költségvetési törvényben önálló költségvetési fejezet képez. Ezen kívül egyáltalán nem kritérium, hogy az adatvédelmi hatóság elnökét az országgyűlés válassza, sőt még az is elfogadott, hogy a miniszterelnök nevezze ki, ha meg vannak függetlenségének a bástyái. Azzal pedig, hogy bírságotlasi joga van a hatóságnak, jobban harmonizálásra került az uniós irányelv.

A kritikai megjegyzéseket nyilvánvalóan lehet bizonyos részletszabályokba tenni, én azt gondolom, hogy az adatkezelés jogalapjainál célszerűbb lett volna átvenni teljes egészében az Irányelv szabályait, most, hogy a kötelezettségszegési eljárás megoldódik, mindenesetre javasolni fogom a törvény felülvizsgálatát. Vannak olyan szabályok, melyeket be lehetne ültetni a magyar jogba, akár megelőző, vagy kísérleti jelleggel, pl: meghatározhatnánk azokat a fontos szektorális adatkezeléseket, ahol az adatvédelmi incidenseket be kéne jelenteni az adatvédelmi hatóságnak egy gyors reakálási lehetőség miatt.

Azt gondolom, hogy alapvetően a szabályzás nem rosszabb, mint a korábbi, sőt jobban harmonizált. Egy valamiben kevesebb: nincs közvetlenül AB- hoz fordulási lehetőség, csak az alapjogi biztoson keresztül, de tudomásul kell venni, hogy az adatvédelmi hatóság egy teljes alkotmányos reform részeként jött létre. Ez egy olyan változtatás, ami kétségkívül kevesebb, azonban az eltelt időszak alatt *(2012.01.01 óta működik a NAIH)* nem tapasztaltuk ennek a negatív hatását.

Összefoglalásul akkor miért mondhatjuk, hogy a közigazgatási hatóság- NAIH- jobb, mint az adatvédelmi biztos rendszer?

Jobb, hiszen a bírságotlasi joggal hatékonyabban fel tud lépni. Noha azt mondjuk, hogy a bírság értéke nem olyan magas „csak” 10 millió forint, de azért nem is kevés, valamint ha megnézzük az új EU szabályozás, az adatvédelmi reformcsomag is a bírságotlást erősítene.

Biztos, hogy jobb ez a konstrukció. Az új szabályozás szerint csak a szervezetre vonatkozó rész 2/3-os a tv-ben, a többi szabály nem így, ha a jogszabály szövegén kellene változtatni, akkor ezek feles többséggel is meghozhatók.

Miért szükséges, hogy az adatvédelemnek külön intézménye, biztosa, képviselője legyen?

Az adatvédelmi ombudsmanoknak mindig is fontos és egyben nehéz szerepük volt. Ha megnézzük az évek során a legnagyobb figyelem mindig az adatvédelmi biztosok megválasztása körül volt. Nyilvánvaló, hogy azért, mert az alapjogi biztossal szemben, aki rendkívül sok alapjog védelméért felelős, az adatvédelmi biztos, vagy most a hatóság csak két jogot véd: adatvédelem és információszabadság. Nem tudunk nagyon olyan ügyet mondani, amelyben e két jog ne szerepelne. Az állam működésének átláthatósága, vagy az állampolgárok megvédése, hogy az állam csak olyan mértékbe lássa át őket, amely feltétlenül szükséges... Nos ez rendkívül összetett és jelentős súlyú terület.

Végül miért fontos mind az egyéneknek, mind az államnak, hogy kiemelten figyelmet fordítsanak a személyes adatok védelmére?

Egyszerűen azért, mert az adatvédelmi szabályozás a magánszféra védelme. Miután a magánszféránál egyre jelentősebb hatása van a digitális adatkezelésnek, ezért az adatvédelem a technika fejlődése miatt egyre fontosabb. A szerepe nem csökken, hanem nő, hiszen ma már egy gombnyomással lehet adatokat kezelni. Eddig voltak térfigyelő kameráink, most felmerül az arcfelismerő rendszerek működtetésének a lehetősége. Eddig fizettük az útdíjat fülkében, matricával, de mi lenne akkor, ha most az egész országban rendszámfelismerő trafipaxokon keresztül elektronikus módon fizetnénk? Ez egy teljesen új dimenzió, az adatvédelem kérdése pedig sosem volt még ennyire fontos.

Budapest, 2014.07.31.

Hidvégi Fanny

Mik a TASZ feladatai? Melyek az adatvédelem és információszabadság program célkitűzései?

A Társaság a Szabadságjogokért jogvédő és jogfejlesztő civil szervezet. 1994 óta működünk Magyarországon. Feladatunk az állam és az állampolgárok közti viszony segítése: jogsegélynyújtás, az állam feletti kontroll. A TASZ azért dolgozik, hogy bárki megismerhesse alapvető emberi jogait és érvényesíthesse azokat a hatalom indokolatlan beavatkozásaival és mulasztásaival szemben.

Az adatvédelem témája egy kicsit „kilóg a sorból”, mert nem csak az állami, hanem a privát szektorra is figyelmet fordítunk. Sőt a közeljövőben szeretnénk a programot még inkább kiterjeszteni az online privacy területére, kifejezetten a privát szektorban.

Milyen formában képzelik a program bővítését?

Magyarországon nem az a legnagyobb probléma, hogy az emberek nincsenek tisztában az információs önrendelkezési jogukkal, hanem az emberi jogokkal általában nincsenek tisztában, és nem tartják értéknek, az emberi jogok kultúrája alacsony szinten van a társadalomban.

Mivel a fiatalokat az Internet érdekli a legjobban, az információs önrendelkezési jogokat arra lehetne használni, hogy rajtuk keresztül más alapjogok fontosságára is felhívjuk a figyelmet. . Ezt egy jó kapunak érzem, mert nem elvont, bár elvont jogok vannak mögötte. Ezért úgy gondolom, hogy be kell építeni az oktatásba az online privacy ismereteket. Ha bemegyek egy iskolába és arról beszélek, hogy hogyan állítsuk meg a korrupciót az unalmas (egy darabig legalábbis), viszont ha azt mondom, hogy Facebook, akkor máris érdekes a téma. Az Interneten keresztül lehet csepegtetni olyan gondolatokat, amik elindítják a fiatalokban, hogy az alapjogaik fontosak.

A TASZ eltökélt célja, hogy felvállalja az ismeretterjesztő, oktató szerepet is. Szeretnénk létrehozni ismeretterjesztő blogot, illetve egy csapatot, akik praktikus szolgáltatásokat, megoldásokat nyújtanak. Ezt nem úgy képezem el, hogy közvetlenül mi fejlesztenénk adatvédelem szempontjából hasznos programokat, appokat, inkább összeszednénk, népszerűsíteni jó megoldásokat. A Tor például egy hasznos és elterjedt software, de itthon kevesen ismerik.

Ha röviden kellene megfogalmazni, akkor mit mondana, miért fontos az adatvédelem?

Úgy gondolom, az emberek nagy részének még „nem esett le”, hogy a kvázi- ingyenes Internetes szolgáltatások úgy működnek, hogy a személyes adataikkal fizetnek érte. Erre a tényre mindenképp fel kell hívni a figyelmet.

Melyek azok az alapvető ismeretek, amiket egy Internet használónak mindenképpen tudni kell?

Ez egy nehéz kérdés, mert sok ilyen van. Talán az lenne a fontos, hogy lássák a kapcsolatot a magán szektor és az állam között. Az állampolgároknak meg kell érteniük, hogy amit egy magán szolgáltatóval közölnek, ahhoz az információhoz milyen hozzáférése van az államnak.

Ha csupán arról beszélünk, hogy az online térben hogyan viselkedjen egy Internethasználó, akkor tudni kell: egy Facebook profilt nem lehet törölni, illetve le lehet szedni egy adatot, de az attól a cég birtokában marad, csak a mi profilunkról tűnik el. Az embereknek látniuk kellene, hogy a személyes adataik mennyit érnek egy cégnek és hogy mit kezdenek vele (például tovább adhatják e harmadik félnek) így talán óvatosabbnak lennének.

A gyerekeket külön ki kell emelni, hiszen ezeknek a szolgáltatásoknak a használata egyre fiatalabb generációknál figyelhető meg. Muszáj megértetni velük, hogy milyen információval és hogyan lehet visszaélni. Meg kell tanítani a biztonsági és adatvédelmi beállítások lényegét, illetve meg kell említeni, hogy bizalmas adatokat (pl.: szülei fizetése) ne adjon meg senkinek. Úgy gondolom, hogy nem kell és nem is lehet megtiltani ezeknek a szolgáltatásoknak használatát, mert rengeteg hasznuk is van és az iskolában a gyermek padtársa úgyszólván megmutatja, hogy kell belépni. Ha a szülő tudtán kívül használja a gyermek a közösségi oldalakat, annak még nagyobb veszélye van, ezért inkább tanítani kell őket.

Milyen (online) privacy ügyekkel néznek szembe tipikusan a TASZ-nál?

Nagyon sokféle ügy érkezik be, a téma gyakran összefügg az aktuális társadalmi, közéleti eseményekkel. Ilyenek voltak: a rezsicsökkentés, a kötelező polgári védelemmel kapcsolatos adatbejelentések, illetve visszatérőek az egészségüggyel kapcsolatos bejelentések.

Mit gondol, milyen szerepet játszik a közoktatás az online privacy területén?

Ahogy én látom, már a legkisebb gyerekek is nyomkodják a szülei telefonját, nem összevissza, hanem tudatosan és sok házi feladat elkészítése az általános iskolákban már számítógépen történik. Szerintem mindenképpen foglalkozni kell az adatvédelemmel, akár az általános iskola elejétől. Akár a számítástechnika óra keretében, de nem tartok elképzelhetetlennek egy külön foglalkozást sem az internetes viselkedést oktatására. Ezen kívül az állampolgári ismeretek, valamint a médiaismeret órák során lehetne az információs önrendelkezési jogról tanulni, illetve fogyasztóvédelmi kérdésekre is ki lehet térni. Az amerikai privacy megközelítés alapvetően fogyasztóvédelmi szempontú, ez a jövőben akár nálunk is jobban elterjedhet.

Mi lehet az állam szerepe ebben a kérdésben?

Az államnak maximális felelőssége van az oktatás területén, de egyre inkább jelentősége van annak, hogy a gyerekek ne csak a központi ideológiával szembesüljenek. Adatvédelmi szempontból az állami felelősség magától értetődik a megfigyelések és a központi adatbázisok területén. Továbbá az adatvédelemmel összefüggő jogszabályok általában le vannak maradva

a technológia fejlettségi szintjétől. Érdekes példa az adatmegőrzési irányelv, amit a közelmúltban az EU bírósága megsemmisített, azonban a magyar jogrendszerben még mindig hatályos törvényként van jelen, így a törvényhozás felelőssége, hogy ma Magyarországon az összes szolgáltató az összes forgalmi adatunkat fél évig tárolhatja.

Mi az egyén szerepe az online privacy területén?

Fel kell hagyni azzal az ostoba gondolkodásmóddal, hogy akinek nincs titkolnivalója, annak nem érdekes, hogy milyen adatait szerezhetik meg harmadik személyek. Az élet legszemélyesebb részéről szólnak az online térben létező adataink. Azonban bizonyos adatainkat tudatosan vagy hanyagságból mi magunk bocsátjuk rendelkezésre. Az információs önrendelkezési jog központi része az egyén döntése az adatai, privátszférája határaitól. Az adatokon keresztül az egyénről profilt lehet alkotni, és lehetőség van azt felhasználni vagy akár visszaélésekre is. Ennek több formája is lehet az egyszerű célzott hirdetéstől egészen addig, hogy valakit megzsarolnak egy interneten elérhető információ birtokában.

Az egyéneknek tehát kulcsszerepük van a kérdésben, először is át kell gondolni, hogy kivel és milyen adatokat osztanak meg önként. Ugyanakkor nem lehet az egyénre tolni a felelősséget, hiszen külső személyeknek tiszteletben kell tartaniuk mások alapvető jogait.

Milyen eszközöket lehetne használni, hogy felhívjuk az állampolgárok figyelmét a privacy fontosságára?

Véleményem szerint alapvetően két módszert használhatunk: a riogatást és a trendivé tételt. El lehet rettenteni az embereket megtörtént negatív eseményekkel. Nagyon jó példa erre, ami a Target törzsvásárlói kártyákkal történt.⁸³

Úgy gondolom a második módszer sokkal hasznosabb és pozitív benyomást kelt. A nagy cégek megnyilvánulásain is az látszik, hogy a fogyasztói bizalom visszanyerésére törekszenek. Már nem az a fontos hogy megosszunk minél több mindent a nyilvános térben, hanem minél több időt töltsünk a szolgáltatás használatával. Célzott hirdetés megjelenhet a személyes üzenetek mellett is, cserébe jobbak a privacy beállítások.

Másrészt csak olyan privátszférát erősítő technológiák lehetnek hatékonyak, amik legalább annyira vonzóak, mint azok a szolgáltatások, amiket amúgy igénybe veszünk. Mindaddig, amíg macerás eljárást és erős számítógépes ismereteket igényel egy anonimitást biztosító browser feltelepítése, addig annak a használata nem fog széles körben elterjedni.

⁸³ Id.: <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/> (2014.09.01)

A TASZ rendszeresen készít videókat, amelyek nem csak jogszabályokat magyaráznak el, hanem emberi történeteken keresztül hívják fel a figyelmet egy-egy alapvető jog jelentőségére, adott esetben sérelmére. A privacy fogalom elég megfoghatatlan, ezzel szemben egy fogyatékos emberről szóló történetet sokkal könnyebb filmes eszközökkel megmutatni. Arra törekszünk, hogy az adatvédelmet és az információszabadságot is közérthető formában tálaljuk a nagyközönség számára.

Jelenleg készül egy videó a józsefvárosi arcfelismerő kamerák használatáról. Szeretnénk eloszlatni azt az állam által közvetített tévhitet, hogy a biztonságunk érdekében egyre többet fel kell adnunk a privát szféránkból. Ugyanis ez csupán egy vélt biztonság. A kamerák nem járulnak hozzá önmagukban a közbiztonság növekedéséhez, azokon a területeken pedig, ahol hatásosnak bizonyultak, komplett rehabilitáció történt (lakásprogram, munkahelyteremtés) és nem a kameráknak önmagukban volt köszönhető a bűncselekmények visszaszorulása.

Mi a véleménye a társadalmi célú hirdetésekről és az online privacy kampányokról?

Azt szokás mondani, hogy minél inkább képi a tartalom, annál könnyebben jut el az üzenet. A Snowden-ügy kapcsán egyre több figyelmet kap az internetes magánszféra védelmének jelentősége. Szuper online kampányok vannak, elérnek kattintásokat, lájkokat, figyelemfelkeltőek. A kérdés csak az, hogy hogyan lesz egy ilyen kampánynak gyakorlati hatása, mert az, hogy megnézek egy videót, nem azt jelenti, hogy utána másképp fogok gondolkodni a kérdésről, sőt másképp is járok majd el a jövőben. Lépéseket kell tenni, hogy a mindennapjaink része legyen. Nem az a lényeg, hogy a kampány hatására egyszer megnyomok egy gombot, hanem az, hogy értékesnek tartom a személyes adataimat.

Ha nem egy országos kampányban gondolkodunk, akkor milyen praktikus megoldások lehetnek? Sokan vannak, akik most kezdik az Internet használatot, de a közoktatásból már kiestek, nekik milyen eszközök lehetnének figyelemfelkelőek?

Ez nem adatvédelem, de adatbiztonság: néhány bank webes vásárlásokhoz Internetkártya használatát teszi lehetővé, ezt igazán hasznosnak tartom. Valamint, a külföldi médiában sokkal nagyobb nyilvánosságot kapnak az online privacy ügyek. Kint ezek Snowden óta folyamatosan címlapon vannak, ismert blogok épülnek körük, ez itthon kevésbé jellemző. Jó lenne, ha olyan magazinok megjelenének magyarul is, mint a Wired.

El tudnám képzelni, hogy a Barátok Közt-be beleírnának egy jelenetet, ami felhívja a figyelmet az online privacy témakörére, így több millió embert el lehetne érni. Én abban látok reményt, hogy az állampolgárok először megnézik, az adott cég mennyi privát szférát kínál,

és ez alapján választanak szolgáltatást. Viszont először a nagy cégeket kell érdekeltté tenni ebben a kérdésben, ez pedig csak úgy működik, ha van rá kereslet. Főleg a Snowden ügy óta, most már (szerencsére) versenytényező az adatvédelem és a magánszféra. Úgy vélem ezzel jár a legjobban minden fogyasztó.

Nagyon érdekes, hogy sok adatvédelemmel foglalkozó szakmabeli elkezdte feszegetni azt a kérdést, hogy azok a kevesek, akik tudatosak az Internet használatában olyan szolgáltatásoknál, amelyek ingyenesek, de cserébe az adatvédelmi beállításaik igen rosszak, fizetnének a jobb privacy beállításokért. Ezzel a TASZ egyáltalán nem ért egyet, hiszen az információs önrendelkezési jog olyan alapjog, amit garantálni kellene, nem pedig megvásárolni. Az lenne a kívánatos, hogy mindenkinek ugyanazok a jogok jussanak, ellenkező esetben csak nő a „gap” a felhasználói csoportok között.

Budapest, 2014.08.

Kutatáshoz használt kérdőív

ADATVÉDELMI ISMERETEK FELMÉRÉSE

1. Neme *

Férfi/ Nő

2. Életkora (év) *

- 15-19
- 20-24
- 25-29
- 30-34
- 35-

3. Legmagasabb iskolai végzettsége *

- Általános iskola
- Szakközépiskola
- Szakközépiskola érettségivel
- Gimnázium
- Egyetem (BA képzés)
- Egyetem (MA képzés)
- Főiskola

4. Az alábbi multimédiás eszközökkel rendelkezem * (több lehetőség is választható)

- okostelefon
- táblagép
- laptop
- PC
- Egyéb:

5. Ha rendelkezik okostelefonnal, mely alkalmazásokat használja rendszeresen? * (több lehetőség is választható)

- nem rendelkezem okostelefonnal
- Facebook
- Facebook Messenger
- Viber
- Foursquare
- Instagram
- Skype
- Egyéb:

6. Regisztrált felhasználója valamely közösségi portálnak? *

Igen/Nem

7. Ha rendelkezik közösségi portál profillal (regisztrált felhasználó), mennyire igazak Önre az alábbi állítások? (ha nem rendelkezik közösségi portál profillal ezt a kérdést hagyja ki)

A következő válaszok közül lehet választani: Igen/Nem biztos/Nem

- Tisztában van azzal, hogy az ismerősei milyen adatait látják
- Tudja, hogyan kell blokkolni az Önt zaklató személyeket
- Tudja, hogyan korlátozhatja bejegyzései nyilvánosságát
- Tisztában van a közösségi oldal adatvédelmi szabályzatával (privacy policy)
- Tudja, hogyan kell adatokat törölnie a közösségi oldaláról

8. Kérem, jelölje be, mennyire igazak Önre az alábbi válaszok! * (rendszeresen: hetente legalább egy alkalommal)

A következő válaszok közül lehet választani: Egyáltalán nem igaz/ Többé-kevésbé igaz/ Teljes mértékben igaz

- Rendszeresen közzétesz olyan fotókat melyeken Ön és/vagy barátai szerepelnek
- Rendszeresen közzétesz olyan videókat melyeken Ön és/vagy barátai szerepelnek
- Rendszeresen közzéteszi tartózkodási helyét (megjelöli azokat a személyeket is, akik Önnel egy társaságban vannak)
- Rendszeresen megosztja, milyen zenét hallgat
- Rendszeresen közzéteszi, milyen filmet néz
- Rendszeresen megosztja, milyen könyvet olvas

9. Kérem, jelölje meg, az alábbi kérdések közül melyek igazak Önre nézve! * (alkalmazások tekintetében melyeket használ)

Igen/Nem

- Ismeri az alkalmazás adatvédelmi szabályzatát?
- Az alkalmazás hozzáfér az ismerősei listájához?
- Az alkalmazás az Ön nevében bejegyzéseket tehet közzé?
- Az alkalmazás hozzáfér az Ön aktuális pozíciójához?

10. Kérem, válasszon!

Igen/Nem

- Előfordult már, hogy visszaéltek az Ön személyes adataival?
- Van olyan ismerőse, akinek személyes adataival már visszaéltek?
- Ismer olyan személyt, aki telefonos/internetes zaklatás áldozatává vált?
- Tisztában van a hatályos magyar adatvédelmi szabályozási rendszerrel?
- Tisztában van azzal, hogy adatvédelmi kérdésekben mely magyar hatóság jár el?
- Tudja, hogy ha személyes adataival visszaéltek, mely Európai Unió hatóságához fordulhat jogorvoslatért?

11. Egy online űrlapon mely adatait adná meg? * (Több lehetőség is választható)

Neve	Bankszámla száma
Életkora	Iskolai végzettsége
Anyja neve	Foglalkozása
Születési helye	Jelenlegi fizetésének nagysága
Születési időpontja	Egészségügyi állapota
Lakcíme	Családi állapota
E-mail címe	Vallási nézetei
Személyigazolvány száma	Politikai nézetei
TB száma	Etnikai hovatartozás

Jogforrások

1949. évi XX törvény a Magyar Népköztársaság Alkotmánya

1977. évi IV. törvény a Magyar Népköztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény módosításáról és egységes szövegéről

1978. évi IV. törvény a Büntető Törvénykönyvről

1989. évi XXXI. törvény az Alkotmány módosításáról

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

1993. évi XCII. törvény a Polgári Törvénykönyv egyes rendelkezéseinek módosításáról

1998.évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

2012. évi C. törvény A Büntető Törvénykönyvről

2012. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2013. évi törvény a Polgári Törvénykönyvről

2/1990. (II. 18) AB határozat, ABH 1990, 18, 22

15/1991. (IV. 13.) AB határozat, ABH 1991, 39, 41.

34/1994. (VI. 24.) AB határozat ABH 1994, 177, 185

15/1995. (IV. 13) AB határozat, ABH 1991, 40.

15/1995. (IV. 13) AB határozat, ABH 1991, 40.

2004/170. BH

OECD, *Guidelines Governing the Protection and Transborder Data Flows of Personal Data*, Paris, 1981 <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> (2014.02.24)

Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, Az egyének védelméről a személyes adatok gépi feldolgozása során című egyezmény, ETS 108, Strasbourg, 1981. Magyarországon kihirdette az 1998. évi VI. törvény <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> (2014.04.12)

95/46/EK irányelv

1/98. állásfoglalás: Platform for Privacy Preferences (P3P) és az Open Profiling Standard (OPS), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp11_en.pdf (2014.04.15)

2000/C 364/01 EU Charter on Fundamental Rights, Nice, 2000

Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union Brussels, 4.11.2010 COM(2010) 609 final http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (2014.03.20)

Convention for the Protection of Human Rights and Fundamental Freedoms CETS No.: 005 <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm> (2014.03.29)

The Freedom of Information Act, 5 U.S.C. § 552, Public Law 89- 554, 80 Stat. 383; enacted 4 July, 1966, Amended 1996, 2002, 2007

Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579, (Dec. 31, 1974)

NY Pub. Off. Law, §87 (2) (b)

Kaye v. Robertson [1991] FSR 62; *The Times* 21 March 1990, *The Independent*, 22 March 1990; *The Guardian*, 22 March, 1990

Bibliográfia

ÁRVA Zsuzsanna (2013): *Kommentár Magyarország Alaptörvényéhez*, Budapest, Wolters Kluwer

BALÁS P. Elemér (1941): „Személyiségi jog” In: **SZLADITS Károly** (ed.) *Magyar magánjog*, Budapest, Grill Károly

BANISAR, David (2001): A privacy védelmének modelljei pp. 9-31 In: *Az odaátra nyíló ajtó= The Door Onto the Other Side*, Budapest, Adatvédelmi Biztos Irodája

BARACSI Katalin (2012): Internetbiztonság Magyarországon és az Európai Unióban In.: *Polgári Szemle* 7. évf. 5-6.sz, febr.

http://polgariszemle.hu/app/interface.php?view=v_article&ID=478 (2014.09.01)

BRANDEIS L. D., WARREN S. (1890): The Right to Privacy, 4 *Harvard Law Review* 193/1890

CHATTERJEE, Deen K. (ed.)(2011): *Encyclopedia of Global Justice* Volume 1-2 Springer, New York etc.

DIETZ Gusztávné dr. Pap Márta (1995): *Adatvédelem, Adatbiztonság* Novorg Kiadó, Budapest

ELLIOTT, Mark THOMAS, Robert (2011): *Public Law*, Oxford University Press, Oxford

FLAHERTY, D. H.: (2001) Privacy és Identitás pp 55-68 In: *Az odaátra nyíló ajtó= The Door Onto the Other Side*, Budapest, Adatvédelmi Biztos Irodája

HATÓ Katalin, F. (2000): *Adatbiztonság, Adatvédelem*, Számalk Kiadó, Budapest

JAKAB András (ed.) (2009): *Az Alkotmány kommentárja*, Századvég, Budapest

JÓRI András (2005): *Adatvédelmi kézikönyv, Elmélet, történet, kommentár*, Osiris Kiadó, Budapest

JÓRI András (ed.) (2010): *Adatvédelem és információszabadság a gyakorlatban*, Budapest: CompLex

KEREKES, Zsuzsa (2001): Az információszabadság az Ombudsman gyakorlatában In: *Az odaátra nyíló ajtó. The Door onto the Other Side*, Adatvédelmi Biztos Irodája

LANDLER M, MARKOFF J (2007): Digital fears emerge after data siege in Estonia. *New York Times*

In.: <http://www.nytimes.com/2007/05/29/technology/29estonia.html> (2014.03.30)

- MAJTÉNYI**, László (ed.) (2005): *Az elektronikus információszabadság*, Eötvös Károly Intézet, Budapest
- MAJTÉNYI** László (2006): *Az információs szabadságok, adatvédelem és a közérdekű adatok nyilvánossága*, Budapest, CompLex
- MAJTÉNYI** László (2010): *Információs és médiajog. 1.-* Miskolc, Bíbor Kiadó
- MCELDOWNEY**, John F. (1998): *Public Law*, Sweet-Maxwell, London
- MORAN** N (2010): Attribution in cyben attacks is difficult, but not impossible, *Secure Nation* (online) In.: <http://securenation.wordpress.com/2010/02/27/attribution-in-cyber-attacks-is-difficult-but-not-impossible/> (2014.03.15)
- PÉTERFALVI** Attila (ed.) (2012): *Adatvédelem és információszabadság a mindennapokban*, HVG-ORAC, Budapest
- QUALMAN**, Erik (2012): *Socialnomics: How Social Media Transforms the Way We Live and Do Business*, John Wiley & Sons Inc., Hoboken, New Jersey
- RAIKKA**, J (2010): Brain imaging and privacy, *Neuroethics* 3, 5-12
- SÁRI** János, **SOMODY** Bernadette (2008): *Alapjogok Alkotmánytan II. 4., átdolgozott kiadás*, Budapest, Osiris
- SCHOEMAN**, Ferdinand D. (ed.) (1984): *Privacy: philosophical dimensions of the literature* In.: *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press
- SMARTT**, Ursula (2006): *Media Law for Journalists*, Sage, London
- SÓLYOM** László (2005): Az adatvédelem és információszabadság jogi előtörténete Magyarországon pp174-183 In: **MAJTÉNYI**, László (ed.) *Az elektronikus információszabadság*, Eötvös Károly Intézet, Budapest
- SZABÓ** Máté Dániel (2005): Kísérlet a privacy meghatározására a magyar jogrendszer fogalmaival. In: *Információs Társadalom* 05/2.
- TRÓCSÁNYI** Sára (2004): *A kommunikáció jogi alapjai*, Osiris Kiadó, Budapest
- WITHMAN**, James Q. (2004): The Two Western Cultures of Privacy: Dignity versus Liberty, *Yale Law Journal*, Volume. 113, April, In.: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=476041 (2014.05.01)