SZABÓ ENDRE GYŐZŐ, RÉVÉSZ BALÁZS

Adataink biztonságban – adatainkban a biztonság?

A magánélet és a biztonság népszerű ellentétpárként tűnhet fel az adatvédelmi gondolkodásban. Leegyszerűsítve olvashatjuk sokszor, hogy ha bizonyos feltételek hiányoznak, aránytalanul nagy áldozatot hozhatunk a személyes magánszféra, a privacy oldalán a biztonság érdekében, és magánszféránk túlzott feláldozása a biztonság oltárán visszafordíthatatlan folyamathoz és orwelli világhoz vezet. Más, a biztonság szempontjait mindenek felettinek hirdető érvelésben viszont a személyes adatok védelmére való hivatkozást alkotmányjogi bűvészkedésnek csúfolják és igyekeznek kisebbíteni a magánszféra-védelem egyébként méltányolandó értékeit. A magánélet és a személyes adatok védelmének pedig nagy a tétje, az adatok illetéktelenek részére való kiszolgáltatása, rosszhiszemű felhasználása egzisztenciákat, családokat tehet tönkre, boldogulási lehetőségeket hiúsíthat meg, ha a védelem alacsony szintre süllyed. Másrészről pedig az információszerzés, illetve előzetes adatgyűjtés a különböző bűnelkövetések, terrorcselekmények előkészületi cselekményei is egyben. Azzal, ha a személyes adataink, magánszféránk védelmében ésszerű lépéseket teszünk, élünk a jog és a technológia adta védelmi lehetőségekkel, adatainkat nemcsak az államtól és a piaci szereplőktől, de a bűnözőktől is elzárjuk, és ezzel mindannyiunk biztonságát szolgáljuk. Egy terület tehát biztosan létezik, ahol a biztonság és magánszféra mezsgyéje összeér: az adatbiztonságé és ezzel összefüggésben a tudatos, felelős felhasználói attitűdé, aminek azonban sokszor az emberi tényező a gátja. Jelen tanulmányban a magánszféra és biztonság kérdéskörének komplexitásáról szólunk, és közös nevezőt keresünk az adatkezelések nézőpontjából, kitérve az új adatvédelmi rendelet (GDPR) magánszféránkat és biztonságunkat egyaránt szolgáló leendő jogintézményeinek bemutatására is.

Kulcsszavak: *adatvédelem, biztonság, magánszféra, adatbiztonság, adatvédelmi incidens*

Szerzői információ:

Szabó Endre Győző, a Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Karának PhD hallgatója. 2002-ben ugyanitt szerzett jogi diplomát, majd két évvel később környezetvédelmi szakjogász oklevelet. 2003-tól az Adatvédelmi Biztos Irodájának munkatársa, 2006-2007-ben másfél évig az Európai Adatvédelmi Biztos mellett nemzeti szakértő. 2011-ben az Európai Unió Tanácsában a magyar elnökség idején az Adatvédelmi Munkacsoport (DAPIX) elnöke. 2012-től a Nemzeti Adatvédelmi és Információszabadság Hatóság elnökhelyettese. Valamennyi budapesti jogi karon, valamint a Szegedi Tudományegyetemen óraadó, magyar és angol nyelven oktat adatvédelmet. Számos könyvrészlet, önálló publikáció fűződik a nevéhez. A Jövő Értelmiségéért Alapítvány Kuratóriumának elnöke.

Révész Balázs, a Nemzeti Közszolgálati Egyetem PhD hallgatója, 2000-ben végzett a Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Karának alapító évfolyamán, ezt megelőzőleg a Kodolányi János Főiskola kommunikációs szakán szerzett diplomát. 2004-től az Adatvédelmi Biztos Irodájának szakértője, 2010-től a Vizsgálati Főosztály helyettes vezetője, 2012-től a Nemzeti Adatvédelmi és Információszabadság Hatóság Vizsgálati Főosztályát, majd 2015. július 1-jétől az Audit- és Információszabadság Főosztályt vezeti. Számos képzésen oktat, köztük az ELTE adatvédelmi szakjogász képzésén, ahol az Információszabadság témakör felelőse. Az adatvédelem és információszabadság körében egyaránt publikál.

Így hivatkozzon erre a cikkre:
Szabó Endre Győző, Révész Balázs, „Adataink biztonságban – adatainkban a biztonság?”.
Információs Társadalom XVII, 1. szám (2017): 45–54.
https://dx.doi.org/10.22503/inftars.XVII.2017.1.3

Szabó Endre Győző – Révész Balázs

Adataink biztonságban – adatainkban a biztonság?

Bevezetés

A magánszféra és a biztonság viszonyának számos dimenziója létezik, hiszen a biztonságot erősítő törekvéseknek egyik legfőbb korlátja a magánszférához és a személyes adatok védelméhez fűződő jog. A személyes adatok védelméhez fűződő jogunk a magánszféra védelmén belül szűkebb, a velünk kapcsolatba hozható adatok, információk rendelkezési jogához kapcsolódik.

A magánszférához való jog fogalma nehezen meghatározható. Alapvetően az emberi személyiség védelmét, a magánélet sérthetetlenségét és a cselekvési autonómiát takarja. Ez tulajdonképpen egy szabadságjog, és mint ilyen, védelmet nyújt a polgárok számára magánéletüknek az állami hatóságok a piaci szereplők és más harmadik személyek általi önkényes zaklatása ellen. Ebben a tekintetben a magánszférához és a biztonsághoz való jog összefonódik: az egyén akkor érezheti magát biztonságban, hogyha egyben szabad is, illetőleg akkor lehet szabad, hogyha biztonságban érzi magát (Révész 2013: 81).

A jogi, társadalmi viták mindig egyik vagy másik rovására próbálnak érvelni és kevéssé törekednek egyensúlyra. E törekvésünkkel van összhangban címválasztásunk, amikor magánélet és biztonság szavak közé nem a „vagy" szócskát illesztjük, hanem az „és"-t. Csábítónak tűnhetne kiélezni az ellentétet a kettő között, ez azonban a jogi elemzés terén most nem célunk. A két terület közötti versengés azért sem célszerű, mert a kiszorítósdiban olyan érvek hangozhatnának el, amelyek mintegy megsemmisíteni igyekeznek a másik oldal érveit.

A múlt hagyatéka a magánszféra-védelem kontextusában

A magánszférához való viszonyunkban az idősebb korú olvasók esetében a kommunizmus keserű tapasztalatai is éreztetik hatásukat. Miközben Nyugat-Európában már a 60-as, 70-es években felismerték azt, hogy az állampolgár személyes adatai és magánszférája akár az állammal szemben is védelemre szorulhatnak, addig a Magyar Népköztársaság államrendszere nagyszámú civilt foglalkoztató besúgóhálózatra épült. Az ezzel összefüggésben feltáruló ismeretek még mind a mai napig mérgeznek emberi kapcsolatokat, ennek ellenére továbbra is, évtizedek múltán is tapintható az igény a tények megismerésére. Az ügynök beszervezése nemcsak önként, a jelölt „hazafias elkötelezettségére" építve történt, de terhelő, kompromittáló adatok alapján is. Kompromittáló adatként olyan anyagokat lehetett felhasználni, amelyeknek nyilvánosságra kerülésétől a jelölt félt, mert családja, hivatali köre, társadalmi kapcsolatai előtt kompromittálódott volna.[1] A megfigyelés során

[1] A beszervezés szabályait az 1956. október 8-án a 94. számú Belügyminiszteri Parancs mellékleteként kiadásra került, és az 1958-ban a belügyminiszter 33. számú parancsával módosított „Az államvédelmi szervek ügynöki munkájának alapelvei" című instrukció képezte.

nem nélkülözték a kor követelményei szerinti fejlett technikai eszközök alkalmazását sem. A 3/a rendszabály a telefonlehallgatásra, a 3/e rendszabály a szobalehallgatásra, míg a 3/r rendszabály a rejtett fotó-, optikai, televíziós berendezésre vonatkozó központi iránymutatást tartalmazta. A cserélt információk gyakran a megfigyeltek magánéletére, vallási meggyőződésére vagy akár szexuális szokásaira vonatkoztak. Az adatgyűjtés nemcsak felnőttektől, hanem a pedagógusok segítségével közvetve az iskolában, a gyerekektől is történt (Révész és Szabó 2013).

A diktatórikus előzményekkel is magyarázható az, hogy a rendszerváltást követően az Alkotmánybíróság (AB) a polgárok magánszféráját teljes mértékben tiszteletben tartva munkálta ki a magyar adatvédelmi szabályozás alapjait, amikor 15/1991. (IV.13.) számú határozatában megállapította, hogy a korlátozás nélkül használható, általános és egységes személyazonosító jel (személyi szám) alkalmazása alkotmányellenes. A nagy mennyiségű összekapcsolt adat, amelyről az érintett legtöbbször nem is tud, kiszolgáltatja az érintettet, egyenlőtlen kommunikációs helyzeteket hoz létre. Előállítható az úgynevezett személyiségprofil, ami az érintett intimszférájába is behatoló művi kép.[2]

Az adatvédelem szempontjából mérföldkőnek számító AB határozat születésekor tehát alapvetően még az állam által megalkotott profil megalkotásának reális veszélye élt a köztudatban és determinálta a testület gondolkodását. Mára azonban leginkább az üzleti szereplők profitorientált érdekei az adatgyűjtés és profilalkotás főbb motivációs tényezői, ennélfogva a felhasználókat, mint fogyasztókat célzó, „személyre szabott" ajánlatok azok, amelyek mögött az érintettek adatainak részletes elemzése áll. A kontroll nélküli adatgyűjtés pedig nemcsak a magánszférát illetően, de a magán- és nemzetbiztonságot illetően is jelentős kockázati tényező, ami ellen tudatosan, felhasználói szinten is célszerű védekeznünk.

A magán és a köz határán

A történelmi rossz emlékek nyomán világosan megfogalmazódik a magánélet igénye. Egy olyan közeg igénye ez, amelyben nem csupán az egyén teljesedhet ki, hanem a szűkebb és tágabb közösséget érintő egyéni döntések szabad mérlegelése is biztosított. Van-e értelme csupán egyetlen ember adatainak védelméről beszélni akkor, amikor az élete összefonódik másokéval? Nyilvánvalóan van, és szükségszerűen ez a jogvédelem kiindulópontja. Az információs önrendelkezés, ahogyan a magyar gondolkodás átvette a német mintát, felelősséget is ró az adatok alanyára. Marad tehát olyan területe az életnek, ami magánügy, még ha ez tipikusan „közös magánügy" is, az egyes ember magánszférájának állapota mások életére is hatással van.

[2] Az AB határozat születésekor még nem, de a mai számítógépes technikák idejében már az egységes személyi szám alkalmazása nélkül is pontos személyiségprofil „varázsolható". Számítógépes programok a publikus internetes oldalakon, közösségi honlapokon közzétett adatok elemzése alapján képesek „jellemrajzot" alkotni az érintettről. Az értékelés alapjául szolgáló adatokat az érintett önként publikálja magáról, ezeket az információkat, kapcsolódó linkeket, az oldalon mutatott aktivitást és több más elérhető tényezőt analizálja a program. Az Európai Unió Bíróságának a Google Spain ügyben hozott 2014. május 13-i döntése (C-131/12) fontos szerepet tulajdonított a profil felépítése lehetőségének akkor, amikor a keresőmotor üzemeltetésének magánszféra-védelmi, illetve adatvédelmi relevanciáját elemezte.

A magánszféra védelmébe beletartozik a birtokvédelem, a magánlakás védelme is. A polgárnak jogában áll kőkerítést emelnie a telke köré és felhívnia a kívülállók figyelmét arra, hogy magánterületére idegenek az engedélye nélkül nem léphetnek be, a személyes adatok védelméhez fűződő joga keretében pedig az adatai bizalmasságának megvédéséért informatikai biztonsági szolgáltatásokat vehet igénybe, adatait nem kőből épített falakkal, hanem a tűzfalon védheti meg.

Meddig lehet a magánélet részletei között kutakodni? Ki húzhatja el a privacy függönyét, meddig léphet be és mit vihet onnan ki? Amíg a kockázatok nem rosszindulatú magatartásból fakadnak, addig a válaszaink minden bizonnyal közel esnek majd a társadalmi konszenzushoz. Az árvíz- vagy éppen földrengés-védelem jól modellezhető jelenségek, nem igényelnek olyan információkat rólunk, amelyek kapcsán ne lehetne meggyőzni mindenkit, hogy ezek gyűjtése, felhasználása szükséges.

A rosszhiszemű magatartások (bűnözés, terrorizmus) esetében már más a helyzet. Az ilyen kockázatok okozói végső soron közülünk kerülnek ki és közöttünk élnek. Ugyanazokon az utcákon járnak, ugyanúgy közlekednek, mint mások, ugyanúgy kommunikálnak és így tovább. Gonosz céljaik elérését az szolgálja leginkább, ha belesimulnak a tömegbe, a statisztikák révén nem lehet kimutatni, hogy kik is ők és pontosan mit csinálnak. Az ilyen személyek és magatartások felkutatása nem történhet meg anélkül, hogy sokan velük együtt a hatóságok látókörébe kerülnének. Ha másként nem, akként, hogy a tipikus magatartások mintázatát az ő viselkedésük elemzése alapján meg lehessen rajzolni.

Mi az, amit itt még el tudunk fogadni? Az életet veszélyeztető kockázatok esetében minden bizonnyal megengedő lenne a közember, mikor akként vélekedik, hogy „kontrollált és elszámoltatható rendszerben pillantsanak be nyugodtan akár a hálószobámba is, ha szükséges." Ez a reakció ahhoz a biztonságpárti elmélethez kapcsolódik, ami szakmai körökben a „nincs mit titkolni", avagy „nothing to hide" néven ismeretes. A szemszögünkből nyilvánvalóan elfogadhatatlan „nincs mit titkolni" elmélet szerint a megfigyelés által a magánszférában okozott kárt kell összemérni az ilyen típusú intézkedések által elérni kívánt céllal. E szerint a biztonság, tekintettel egy demokratikus államban betöltött szerepére, mindig megelőzi a magánszféra védelméhez fűződő érdekeket. Amennyiben tehát egy állampolgárnak nincs mit titkolnia, semmilyen információt nem lehet felhasználni ellene, a magánszférájába történő hatósági beavatkozás ezért nem is okozhat kárt (Révész 2013: 88). Az elv többszörösen is hibás feltételezésen alapul álláspontunk szerint, nem csupán az adatok felhasználásának fázisában, hanem már korábban, az adatok gyűjtése is aggályokat vet fel.

Nemzetbiztonság és biztonság

A biztonságról és a magánéletről folytatott viták metszéspontjában mindig megfogalmazódik a nemzetbiztonság elvárása.

A biztonság az egyik legősibb és legalapvetőbb elvárásunk és jogunk. Központi eleme természetesen az állampolgárok érdekeinek, életének védelme mindenfajta bel- és külföldi veszélyektől. Emellett ugyanakkor a biztonság alkalmazási köre kiterjed minden olyan helyzetre, amelyek hatással lehetnek az állam azon képességére, hogy a nemzet jó-

létét biztosítsa. Az állampolgárok életének védelme és a rendfenntartás mellett így egyike azon alapvető, kollektív nemzeti céloknak, amelyek megvalósítása az államok elsődleges feladata. Ahogy az az Osman v. United Kingdom ügyben született ítélet megfogalmazza: „*Az államokat pozitív kötelezettség terheli a polgáraik életének megóvásáért*".[3] Biztonság nélkül továbbá kivitelezhetetlenné válna az emberi jogok, valamint az egyéni és kollektív érdekek garantálása is. Egy kaotikus, bizonytalan helyzetben lévő országban a demokratikus értékek biztosítása hamar háttérbe szorul. Könnyen belátható tehát, hogy a biztonság érvényesüléséhez kiemelkedő érdekek fűződnek, és ezért jogi védelmet élvez. Az abszolút biztonság elérése azonban csupán utópisztikus vágyálom lehet, arra csupán csak törekedni tudnak az államok.

A magánélet nem lakatlan sziget jellegű élmény, ehhez hasonlóan a legtöbb kockázat esetében a biztonság sem lehet az. A biztonságunkat fenyegető kockázatok feltárása és csökkentése összjátékot igényel a társadalom szintjén. Nyilvánvaló ez a közlekedésben, tűzvédelemben és sok más területen. Van egy pontja a kockázatoknak, ahol már nem a társasházi kamera vagy a riasztó berendezés a hatékony megoldás, és itt lépnek be az intézmények, amelyek aztán a köz (teljes vagy részleges) bizalmát élvezve kezelnek adatokat közös biztonságunk megóvása érdekében.

Az elvárások, az intézményekbe vetett bizalom és az intézmények lehetőségei hármasában úgy tűnik, elérhető valamilyen társadalmi egyensúly. Ez a harmonikus állapot azonban a tapasztalat szerint nagyon rövid életű. Gyakran történik olyan esemény, amely a létezőnek vélt egyensúly valamelyik irányba való felborulását igazolja. A Snowden-féle kiszivárogtatások után az európai közvélemény jogosnak érezte az amerikai kormányon számon kérni a privacy nagyobb tiszteletét. A brüsszeli, a párizsi vagy éppen a nizzai terrortámadás után az a kérdés fogalmazódott meg élesen, hogy miért nem lehetett mindezt megakadályozni? A viták során pedig minden esetben megfogalmazódik az igény az intézmények hatékony működése iránt.

Nem kétséges, hogy erre szükség van. Sőt, el is várjuk, hogy ezek az intézmények hatékonyan működjenek, férjenek hozzá és zavartalanul használhassák azokat az adatokat, amelyek feladataikhoz szükségesek. Egy jogállamban azonban az is jogos elvárás, hogy a biztonságért felelős kormányzati szolgálatok kontroll alatt, végső soron a polgároknak elszámolva teljesítsék kötelezettségeiket. A polgároknak e szervezetekbe vetett bizalma pedig nagyban múlik azon, mennyiben osztják meg a népképviseleti szervekkel és a közvéleménnyel a terrorizmus ellen elért sikereiket. Nem elég az, ha azt mondják, hogy az adatainkra szükségük van, hogy megóvjanak minket, tényszerűen – természetesen anonimizáltan – kommunikálni kell a polgárok számára a terrorizmus elleni harc sikerét azért, hogy ez az együttműködés közös lehessen, és azt érezze a polgár, hogy átláthatóan működnek ezek a szervezetek.[4]

Pusztán jogi szempontból az Európai Unió nem kíván közvetlenül beleavatkozni a tagállamok nemzetbiztonsági mozgásterébe, ugyanis a Szerződések a nemzeti biztonságot

[3] Osman v. the United Kingdom, 28 October 1998, § 115, Reports of Judgments and Decisions 1998-VIII.

[4] Bővebben lásd Révész (2014)

kivonják az uniós jogalkotó hatásköréből.[5] Ennek következménye, hogy a személyes adatok védelméről szóló uniós jogalkotás ezt a területet teljes mértékben figyelmen kívül hagyta. Az Unió azonban nem kerülhette meg a vitát, mert ez Egyesült Államokkal szemben pontosan ezen a területen bonyolódott hosszú és részletes vitába. Az Edward Snowden által kiszivárogtatott, az Egyesült Államok nemzetbiztonsági szerveinek működésébe bepillantást engedő információk kapcsán ugyanis az európai államok a privacy tiszteletére szeretnék rábírni az USA kormányát. Egy olyan vita alakult ki tehát, ahol az EU-nak nincsenek saját standardjai sem, hiszen hatáskör hiányában nem is alkothatott ilyet.

A fogódzót nem is az EU, hanem az Európa Tanács nyújtja. Az Emberi Jogok Európai Egyezményének 8. cikke[6] rögzíti a magánélethez való jogot, amelyet a nemzetbiztonsági területen is érvényesíteni kell.

Magánszféra és technológia

Az új technológiák egyfelől a magánszféra korábban nem látott kibontakozásának lehetőségét kínálják. A kommunikáció, az adatok megörökítése, gondolatok megosztása és sok más az információs és kommunikációs technológiának köszönhető. Azonban ez nem csak a kibontakozás, hanem az adatok rögzítésének korábban elképzelhetetlen lehetőségét is magával hozza, új dimenzióba helyezve a biztonság és magánszféra összefüggéseit.

Úgy tűnik, hogy az adatgyűjtés terén az ütemet nem a biztonsági kockázatok megjelenése, hanem a technológia által kínált rögzítési módozatok adják. A „technológiai determinizmus" ilyen értelemben tehát alapvetően hat ki a különböző érdekek egyensúlyára (Irion 2016), és a technológia nem elsősorban búvóhelyet jelent, hanem a magatartásokat követhetővé tevő közeggé is válik. Nyitva marad a kérdés, vajon van-e ideális határvonal a biztonsági kockázatok feltárása és a magánélet védelme között? A rosszhiszemű magatartások esetében valószínűleg egyértelmű érv adódik: ezekben az esetekben a biztonság szavatolása érdekében a lehető legszélesebb körű lehetőségekre tartanak számot az illetékes szervek, hiszen ez adódik az ilyen jellegű bűnözés természetrajzából.

A biztonsági incidensek egyike, az adatvesztés nemcsak szándékos külső beavatkozások (hacker-, vírustámadás), hanem sok esetben a munkavállaló hanyagsága, gondatlansága miatt következik be. A statisztikák szerint a cégek, szervezetek adatvesztése nagy százalékban erre az okra vezethető vissza. Az adatvesztés megelőzése érdekében hatékony titkosítási és erős hozzáférés-ellenőrzési megoldásokat célszerű használni, mivel a mobil-

[5] Az Európai Unió Működéséről szóló Szerződés 4. cikk (2) bekezdése szerint „Az Unió tiszteletben tartja a tagállamoknak a Szerződések előtti egyenlőségét, valamint nemzeti identitását, amely elválaszthatatlan része azok alapvető politikai és alkotmányos berendezkedésének, ideértve a regionális és helyi önkormányzatokat is. Tiszteletben tartja az alapvető állami funkciókat, köztük az állam területi integritásának biztosítását, a közrend fenntartását és a nemzeti biztonság védelmét. Így különösen a nemzeti biztonság az egyes tagállamok kizárólagos feladata marad."

[6] 8. cikk 1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. 2. 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 megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.

eszközök és internet-alkalmazás elterjedése sebezhetőbbé tette az adattárolási rendszereket. Az online szolgáltatások és távoli hozzáférések bővülésével „biztonsági rések" keletkeznek. E biztonsági rések rosszindulatú kihasználásának esélyét növeli a munkavállaló, felhasználó tapasztalatlansága, hanyagsága, ezért is fontos a munkatársak oktatása és az adatbiztonsági előírások betartatása (Révész 2012).

Emberi sajátosság, hogy azt érezzük biztonságban, ami felett szabadon rendelkezhetünk, és akkor érezzük magunkat biztonságban, ha szabadon cselekedhetünk és befolyásunk lehet életünk alakulására. Van, aki fél, ha más autójába ül, és más vezeti az autót, de nem aggódik, ha nála a kormány, pedig lehet, hogy rosszabbul vezet, mint az, akinek nem bízik a vezetési tudásában. Így vagyunk valamelyest az új technológiákkal is.

Az, hogy a félelem erősebb az adataink védelme iránti elkötelezettségünknél, annak tudható be, hogy a félelem érzése agyunk felsőbbrendű részében keletkezik. A kényelem pedig azért tud győzedelmeskedni az adatvédelmi megfontolások fölött, mivel míg komfortérzetünk bekövetkezése valóságosan és azonnal érezhető, az adataink védelmének hiányosságából fakadó károk sokkal kevésbé megfoghatóak és csak hosszabb idő elteltével éreztetik hatásukat (Schneier 2016).

A ma népszerű generációs felosztás szerinti korcsoportok, nevezetesen a veteránok, a Baby boom és X generáció, de még sokszor az Y generáció tagjai sem mozognak komfortosan az új technológiák világában és nem alkalmaznak privátszférát erősítő technológiákat (Privacy Enhancing Technologies, PET). Ennek a helytelen attitűdnek az okai sokrétűek. Egyrészről abból a téves feltevésből adódnak, hogy a szigorú törvényi előírások online környezetben is visszatartó erővel bírnak, másrészről abból a könnyelmű hiszékenységből táplálkoznak, hogy a szolgáltatók nem gyűjtenek róluk személyhez társítható formában adatokat vagy azt mindig a törvényi előírásokat követve szabályszerűen teszik. Legtöbbször persze a kényelmi szempontok azok, amelyek miatt fittyet hánynak az alapvető óvintézkedésekre, így például okostelefonon a képernyőzár használatára, vagy arra, hogy ismeretlen nyílt wifi rendszeren keresztül ne nyissák meg a munkahelyi e-mailjeiket.

Még a tudatosabb felhasználókkal is gyakran előfordul, hogy egy-egy alkalmazás letöltésekor észlelt kezdeti problémák okán inkább eltekintenek ezek használatától. Az adatbiztonság nem önmagában és más tényezőktől függetlenül létezik. Egy rendszer biztonsága nagyban függ a felhasználók magatartásától, például attól, hogy hajlandóak-e biztonsági alkalmazások futtatására eszközeiken vagy legalább a jelszóválasztásnál eleget tesznek-e a karakterhosszúságra, kis/nagy betű választásra, az időszakonkénti jelszóváltásra vonatkozó „alapszabályoknak", avagy a kényelmi szempontok és a nemtörődömség okán megspórolják ezeket az erőfeszítést egyébként nem igénylő óvintézkedéseket.

Az Adatvédelmi Irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport 5/2009. számú véleményében az ismertségi hálózatok, közösségi oldalak kapcsán az adatvédelmi beállítások jelentőségére hívja fel a figyelmet és a hozzáférés gondos kialakítására koncentrál. Kiemeli az üzemeltető/szolgáltató felelősségét annak apropóján, hogy mivel az alapértelmezett beállításokon a regisztrált felhasználók csak kisebb hányada változtat és differenciálja a hozzáférést adataihoz, ezért a szolgáltatónak kellene az alapbeállítást a személyes adatok védelmével összhangban kialakítania. A Munkacsoport elvárásként fogalmazza meg, hogy a szolgáltatóknak olyan alapértelmezett beállítást kellene nyújtaniuk, amely a külső látogató számára redukált hozzáférést tesz csak lehetővé, és az adat-megismeréshez a felhasználó kifejezett hozzájárulása szükséges minden olyan esetben, mikor

az ismertségi körön kívüli személy kíván a profilt alkotó információhoz hozzáférni. A Munkacsoport ideálisnak tartaná, ha a korlátozott hozzáférésű profilokat elzárnák a belső keresőmotorok elől, az életkor, lakhely, vagy más hasonló paraméterek szerinti keresési lehetőségeket is beleértve. A hozzáférés kiterjesztésére vonatkozó döntések pedig nem lehetnének hallgatólagos jellegűek, például oly módon, hogy az ismertségi hálózat kezelője „elutasítási" lehetőséget biztosít (Révész 2012).

Az Európai Unió standardja: megfelelő védelmi szint a személyes adatok védelme tekintetében

Az Európai Unió az Egyesült Államokba irányuló adattovábbításokat a saját adatvédelmi szabályai szerint kontroll alatt kívánja tartani. A célkitűzés lényege, hogy az Unióban érvényesülő védelmi szintet alapul véve az Unióban tartózkodók magánszféráját abban az esetben is tiszteletben kell tartani, ha az adatok az Európai Unió területét elhagyják[7]. Ezt a védelmi szintet az Egyesült Államok (és más harmadik államok) viszonylatában is meg kell határozni, annak ellenére, hogy az Unió maga ilyen „védelmi szintet" a nemzetbiztonsági ügyek terén nem tud felmutatni.

A vitát az tette időszerűvé, hogy a Snowden-féle kiszivárogtatások után egy panaszos megkérdőjelezte az adatok védelmét az amerikai oldalon. Kérelmének középpontjában pedig a védelmi program átláthatatlansága, és az ezzel kapcsolatos kételyek álltak. A konkrét ügyben az Európai Unió Bírósága arra a következtetésre jutott, hogy az EU adatvédelmi hatóságait nem lehet megfosztani attól a lehetőségtől, hogy az adatok harmadik államba való továbbítása kapcsán a megfelelő védelmi szintet elemezhessék. Ennek hiányában az Egyesült Államokba irányuló adattovábbítások kerete nem lehet jogszerű.[8]

A 2015. október 6-án érvénytelenné nyilvánított jogi keret, a Safe Harbor helyébe lépett 2016-ban az úgynevezett Privacy Shield (Adatvédelmi Pajzs) megállapodás.[9] A korábbi hiányosságok a nemzetbiztonsági célú adatgyűjtések kapcsán adódó kérelmek (például tájékoztatás nyújtása) intézésére is irányul, ezért témánk szempontjából is meghatározó, hogy miként vizsgázik a gyakorlatban az új keret.

[7] Az EU adatvédelmi szabályozása az Európai Gazdasági Térségre is kiterjed, így az Norvégia, Izland és Liechtenstein tekintetében is alkalmazandó.

[8] Az Európai Unió Bírósága 2015. október 6-án kelt ítéletében kimondta: az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló, 2000. július 26-i 2000/520/EK bizottsági határozat, amelyben az Európai Bizottság megállapítja, hogy valamely harmadik ország megfelelő védelmi szintet biztosít, nem akadályozza meg azt, hogy az ezen módosított irányelv 28. cikke szerinti tagállami felügyelő hatóság megvizsgálja a személy által benyújtott, valamely tagállamból e harmadik országba továbbított és őt érintő személyes adatok kezelése vonatkozásában a jogainak vagy szabadságainak védelmével kapcsolatos kérelmet, amennyiben e személy arra hivatkozik, hogy az ezen országban hatályos jog és gyakorlatok nem biztosítanak megfelelő védelmi szintet.

[9] Az Európai Bizottság 2016. július 12-én fogadta el döntését a Privacy Shield által biztosított megfelelő védelmi szintről az Amerikai Egyesült Államok vonatkozásában.

Az új adatvédelmi rendelet biztonságunkat és információs önrendelkezésünket erősítő jogintézményei: adatvédelmi incidens és adathordozhatóság

Az Európai Parlament és a Tanács 2016/679 rendelete[10] amit szakzsargonban csak GDPR-ként említenek[11], az adatvédelem európai és a hazai történetének új mérföldköve. A rendelet számos ponton csak az adatvédelmet érintő alapvető elvek és megoldások újragondolását és fogalmilag új definíciók rendszeresítését hozza, néhány vonatkozásban azonban érdemi újítással gazdagítja és erősíti is az adatvédelmi mechanizmusokat. Az új technológiák és az adatbiztonság szempontjából két jogintézmény e tanulmány kontextusában is feltétlenül említésre méltó: az adatvédelmi incidensek jelentési kötelezettsége és az adathordozhatóságé.

Az adatvédelmi incidens fogalmát 2015. október 1-jétől az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) is tartalmazza, tág körre vonatkoztatva a személyes adat bármely jogellenes kezelését vagy feldolgozását, így különösen a jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést, valamint a véletlen megsemmisülést és sérülést is értve ez alatt.[12]

A gyakorlatban azonban az adatvédelmi incidensek vezetésének akkor van jelentősége, ha az esemény jelentős hatásokat generál, annak nagyszámú elszenvedője van (például több ezer banki ügyfél), különleges adatokról van szó (egészségügyi intézmény betegadatai) vagy egy üzem, üzletág adatbiztonságát érinti. Az incidens bejelentése a fokozatosság elvének mentén az adatkezelő belső nyilvántartását, a tagállami adatvédelmi hatóság értesítését és végső soron az érintettek tájékoztatását jelenti. Az intézmény bevezetése mögött az a vitathatatlanul pozitív szándék húzódik, hogy amennyiben ezeket az adatvesztéseket késlekedés nélkül jelentik be a hatóságnak, úgy a szakértőknek még van ideje arra, hogy mentse, ami menthető. Lényegében egyfajta kármentési védelmi mechanizmus beépítéséről van szó, a fokozatosság kritériumát is szem előtt tartva.

A jogalkotó szándéka szerint az incidensek bejelentése révén el lehet kerülni, illetve enyhíteni lehet azokat a kockázatokat, amelyek a következőkben nyilvánulnak meg: a természetes személyeket érhető fizikai, vagyoni és nem vagyoni károk; az, hogy személyes adataik felett elveszíthetik a rendelkezésüket, jogaikban korlátozhatják őket, személyazonosság-lopás vagy személyazonosság-visszaélés áldozatai lehetnek, az álnevesítést jogosulatlanul feloldhatják, a jó hírnevük sérülhet, a szakmai titoktartás alá eső adatok elveszíthetik bizalmas jellegüket, vagy egyéb gazdasági vagy szociális hátrányt szenvedhetnek. Az adatvédelmi intézkedés tehát mindezeket a lehetséges társadalmi következményeket szem előtt tartva érvényesítendő (Szabó 2016).

Valószínűsíthető, hogy jelenleg számos incidens látens marad, hiszen a piaci szereplők a spontán üzleti érdekeiktől vezérelve nem kürtölik világgá adatvesztéseiket, mert anyagi veszteségektől tartanak, és úgy vélik, aláásnák az irántuk felépített ügyfélbizalmat. A jelentős incidensek titokban tartása, majd megtörténtének véletlen napvilágra kerülése azon-

[10] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK számú irányelv hatályon kívül helyezéséről.

[11] A General Data Protection Regulation rövidítéseként, GDPR.

[12] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 26. pontja.

ban nagyobb bizalomvesztést okozhat.

Az érintetteket az adatkezelő „indokolatlan késedelem" nélkül köteles értesíteni, kivéve akkor, ha az elvesztett adatok mások számára értelmezhetetlenek, vagy az érintetteket fenyegető kockázat valószínűsíthetően nem valósul meg, avagy az érintettek tájékoztatása aránytalan erőfeszítéssel járna.

A hatóság szakértői az incidensről való értesülés után értékelik a helyzetet, rekonstruálják a történteket, és a további adatveszteség megakadályozása érdekében intézkedéseket javasolnak és megteszik a szükséges lépéseket. Amennyiben az érintettek tájékoztatása valamely okból elmaradt, de az incidens súlya, kritikus szintje indokolja, a hatóság az érintettek értesítéséről is rendelkezik.

Az „adathordozhatóság", mint az érintett új jogosultsága, már a modern környezetben, a felhők (cloud computing) és okos eszközök világában ragadja meg, megfogalmazásában is találóan az információs önrendelkezés lényegi tartalmát: azt, hogy személyes adatainknak, mint a hozzánk tartozó „csomagnak" az útját mi magunk határozzuk meg. E jogunk gyakorlása feltételezi a szolgáltatók, alkalmazások közötti interoperabilitást, azaz az átjárhatóságot. Az Európai Unió jogának, az európai közigazgatások közötti átjárhatósági eszközökről szóló 2009/922/EK határozatában foglaltak szerint az átjárhatóság az eltérő és különböző szervezetek együttműködési képessége a kölcsönösen hasznos és kölcsönösen megállapított közös célok érdekében, ideértve az információk és ismeretek megosztását a szervezetek között az általuk támogatott munkafolyamatokon keresztül, a saját információs és kommunikációs rendszereik közötti adatcsere lehetőségével.

Az adathordozhatóság ugyanakkor nemcsak technikai, hanem további jogi kérdéseket is felvet: „adatcsomagjaink" a szövevényes kommunikáció hálójában nem egymástól függetlenek, egy adott személyes adatállomány más személyek adatait is tartalmazza, akik nem feltétlenül szeretnék, ha adataik más szolgáltatóhoz vándorolnának. Erre az esetre a rendelet azt az iránymutatást adja, hogy „ha egy adott személyes adatállomány egynél több érintettre vonatkozik, a személyes adatok védelméhez való jog nem sértheti az egyéb érintettek e rendelet szerinti jogait". Nem adódhat tehát olyan helyzet, amelynek eredményeként az adathordozás révén más érintett hátrányosabb helyzetbe kerül (Szabó 2016).

Összegzés: a társadalmi optimumra törekedve

A magánélet és biztonság vonatkozásában felvetett kérdések nyitottak maradnak, de a társadalmi optimum keresése ezt meg is kívánja. Az Unió új, hatásosnak ígért megoldásokkal kísérletezik, de a realitás az, hogy nincsen olyan keret- és intézményrendszer, és nem valószínű, hogy valaha is meg fog születni az a tökéletes intézkedés- és intézmény-együttes, amely a magánélet és a biztonság kérdését végérvényesen és megnyugtatóan önmagában rendezné. A kérdéseket újra meg újra fel kell tenni, ha szükséges, újra kell fogalmazni. A problémakör komplex, akár az emberi tényező, az állam szerepe vagy a jogi eljárások és technika oldaláról közelítünk hozzá.

A magánélet jelentőségét megértő, a védelmet megkövetelő hozzáállás alapvető a biztonsághoz vezető válaszok megtalálásához. Az egyént és a közösséget fenyegető kockázatok megoldásához tulajdonképpen mindenkinek a közreműködésére szükség van. Témánk szempontjából ez azt jelenti, hogy a rosszindulatú magatartásokat kiszűrni képes hatóságok számára

megadjuk a bizalmat, ugyanakkor beszámolási kötelezettségük teljesítése mellett alapjogi korlátok közé tereljük működésüket. A felelősség közös: uniós, tagállami és egyéni. Az adatbiztonság pedig mindkét cél, a biztonság és a személyes adataink védelmét is szolgálja.

Irodalom

A 29. cikk alapján létrehozott Adatvédelmi Munkacsoport 5/2009. számú véleménye az internetes ismertségi hálózatokról, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_hu.pdf

Irion, Kristina, "Accountability unchained: Bulk data retention, preemptive surveillance and transatlantic data protection", in Marc Rotenberg, Julia Horwitz and Jeramie Scott (eds.), *Privacy in the Modern Age: The Search for solutions,* The New Press, New York, London, 2016, pp. 78-92.

Révész Balázs, „Adatbiztonság", in Péterfalvi Attila (szerk.), *Adatvédelem és információszabadság a mindennapokban*, HVG ORAC, Budapest, 2012.

Révész Balázs, „Magánszféra kontra biztonság – egyensúlyra törekedve", in *A terrorizmus Rubik kockája, avagy a fenyegetések komplex megközelítése* konferencia-kötet, Nemzetközi tudományos-szakmai konferencia, Budapest, Duna Palota 2013. szeptember 30., Belügyminisztérium Oktf, 2014.

Révész Balázs és Szabó Endre Győző, „Adatvédelmi jogi ismeretek", in Christián László (szerk.), *Az információs társadalom jogi vetületei – Alkalmazott jogi informatika*, PPKE JÁK, Budapest, 2013.

Schneier, Bruce, "Fear and convenience in Privacy in the modern age", in Marc Rotenberg, Julia Horwitz and Jeramie Scott (eds.), *Privacy in the Modern Age: The Search for solutions,* The New Press, New York, London, 2016, pp. 200-203.

Szabó Endre Győző, „Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről I.", *Pázmány Law Working Papers* 2016/26.

Szabó Endre Győző, „Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről II.", *Pázmány Law Working Papers* 2016/27.